Freedom and Regulation on the Information Superhighway

A study of the Internet Content Rating System in South Korea

You-Seung Kim

A thesis submitted to the University of London in fulfilment
for the award of a Doctor of Philosophy Degree

School of Library, Archive, and Information Studies
University College London
University of London

2004

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

This PhD thesis aims to explore issues relating to Internet content regulation and the methods of dealing with illegal and harmful content on the Internet. Firstly, the thesis begins with a discussion of the theoretical issues relating to freedom and regulation on the Internet. Debates over freedom of expression and governmental regulation on the Internet are critically appraised through case studies in the US, Australia, China, the UK and the EU. Furthermore, the notion of Internet self/co-regulation and its advantages and drawbacks are considered. Issues relating to the implementation of co-regulation regarding Internet content are also explored.

Secondly, detailed technical reviews and critiques of the Internet content filtering and rating systems are conducted. Two US legal cases that deal with filtering software issues are discussed. Ten stand-alone filtering software products are reviewed in order to examine how the filtering technologies are applied to commercial products in practice. Three leading Internet content rating systems are also examined.

Thirdly, close attention is paid to Internet content regulation in South Korea. Its significant Internet usage and infrastructure are explored. A mandatory Internet content rating system in use in South Korea is analysed and situated within a broader context. Its impacts on actual Internet contents are researched through case studies and a survey.

The thesis concludes by examining the theoretical potential for better solutions to the controversial issues of freedom of expression and regulation on the Internet. Finally, a number of policy proposals concerning Internet content regulation are critically discussed and a number of recommendations are made.

ABSTRACT 2
LIST OF ABBREVIATIONS 10
LIST OF TABLES 13
LIST OF FIGURES 15

CHAPTER 1
INTRODUCING THE INTERNET

1.1. Introduction 17
1.2. The Emergence of the Internet 20
1.3. The Nature of the Internet 24
1.4. The Literature on Internet Regulation:
A Utopian Vision and a Digital Panopticon 29
1.5. Regulating Information on the Internet 36

CHAPTER 2
FREEDOM OF EXPRESSION AND REGULATION ON THE INTERNET

2.1. Declarations and Conventions on Freedom of Expression 46
2.2. Responsibilities of Freedom of Expression 50
2.3. The Internet is not a Legal Vacuum 54
2.4. Regulating Illegal and Harmful Content on the Internet 57
2.4.1. Illegal Content and Harmful Content 57
2.4.2. Illegal Content 58
2.4.3. Harmful Content 60
2.5. Freedom of Expression in South Korea 62
2.6. Governmental Internet Regulation 71
2.6.1. The US 72
2.6.1.1. The Communications Decency Act 1996 73
2.6.1.2. The Child Online Protection Act 1998 79
2.6.1.3. The Implications of the CDA and the COPA 82
2.6.2. Australia 84

2.6.2.1. The Broadcasting Services Amendment (Online Services) Act 1999 84
2.6.2.2. The Features of the Australian Internet Content Regulation 87
2.6.2.3. A Critique of the Australian Internet Content Regulation 88
2.6.3. China 90
2.6.3.1. China: Internet Legislation 1996-2000 91
2.6.3.2. Technical Measures for Controlling Internet Content in China 93
2.6.3.3. A Modern Paradox in China 95
2.6.4. The EU and the UK 97
2.6.4.1. The UK: Governmental Regulation against Obscene Internet Content 98
2.6.4.2. The Development of the EU Internet Content Policy 101
2.7. A Comparative Analysis of Governmental Internet Content Regulation 106
2.8. Beyond Governmental Internet Regulations 108

CHAPTER 3

SELF-REGULATION ON THE INTERNET

3.1. Introduction 111
3.2. The General Definition of Self-Regulation 111
3.3. Self-Regulation of Internet Content: Definition and Aims 114
3.3.1. Advantages of Internet Content Self-Regulation 117
3.3.2. A Critique of Internet Content Self-Regulation 119
3.4. Co-Regulation of Internet Content 121
3.5. Implementation of Internet Content Co-Regulation: The Safer Internet Action Plan 122
3.6. Internet Content Self-Regulatory Institutions in Europe 126
3.6.1. The Internet Watch Foundation, UK 127
3.6.2. INHOPE 130
3.7. Conclusion 132

CHAPTER 4

THE FIRST GENERATION FILTERS

4.1. Introduction 135
4.2. Technical Aspects of First Generation Filtering Software 136
4.2.1. Definition 136
4.2.2. Methods of Filtering 137
4.2.3. Locations of Filtering 139
4.3. Technical Review: 10 Examples of Commercial Filtering Software 141
4.3.1. Filtering Coverage 143
4.3.2. Filtering Methods 145
4.3.3. Reporting 149
4.3.4. Customisability 150
4.3.5. Usability 153
4.3.6. Effectiveness 157
4.4. A Critique of First Generation Filtering 164
4.5. Free Speech Rights Issues of Filtering Software on the Internet 168
4.5.1. Case Study: Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, Virginia, 1998 170
4.5.2. Case Study: The Children's Internet Protection Act, 2000 173
4.6. Conclusion 179

CHAPTER 5

THE INTERNET CONTENT RATING SYSTEM

5.1. Introduction 183
5.2. Internet Content Rating System: Technical Specification 183
5.2.1. PICS 183
5.2.2. PICSRules 192
5.2.3. RDF 194
5.3. Internet Content Rating System: Technical Analysis 196
5.3.1. The SafeSurf System 197
5.3.2. The RSACi System 199

7.1.3. JEONGBO TONGSINMANG IYONG CHOKJIN MIT JEONGBO BOHO DEUNGE GWANHAN BEOPYUL [Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.] 248
7.1.3.1. Article 31 and the Internet Content Rating System 249
7.1.3.2. Article 42 and the Indication Method for Harmful-to-youth Content on the Internet 253
7.2. Technical Review: Two Internet Content Rating Systems of the ICEC 255
7.2.1. SafeNet Internet Content Rating System 256
7.2.2. The Harmful-to-youth Material Indication System 260
7.3. A Critique of ICEC Deliberation 265
7.4. A Critique of ICEC Third-Party Rating 269
7.5. Conclusion 270

CHAPTER 8

THE IMPACTS OF THE INTERNET CONTENT RATING SYSTEM ON THE ACTUAL INTERNET CONTENTS IN SOUTH KOREA

8.1. Introduction 274
8.2. Case Study I: EXZONE.COM 274
8.3. Case Study II: iNOSCHOOL.NET 284
8.4. Rating and Removal Orders 288
8.5. Questionnaire Analysis 290
8.5.1. Introduction 290
8.5.2. Section I: General Information 291
8.5.3. Section II: The Internet Content Rating System 292
8.5.4. Section III: The Harmful-to-youth Medium Material Indication System 299
8.5.5. Section IV: Labelling and Rating 304
8.5.6. Findings 313
8.6. Conclusion 314

CHAPTER 9

A STEP TOWARDS THE NEW INTERNET CONTENT REGULATION IN SOUTH KOREA

9.1. Introduction 318
9.2. Article 53 of the Telecommunications Business Act and the Korean Constitutional Court 318
9.3. Reformed Bill of Article of the Telecommunications Business Act 322
9.4. Co-Regulation of Internet Content and South Korea 325
9.5. The Absence of the Self-Regulation System in South Korea 327
9.6. Towards the New Internet Content Regulation 329
9.6.1. A Role of the Government 329
9.6.2. Responsibilities of the Internet Industry 332
9.6.3. Empowering End-Users 336
9.7. Conclusion: The Korean "R3 Net" Strategy 337

CHAPTER 10

CONCLUSION: THE FUTURE OF INTERNET CONTENT REGULATION

10.1. Introduction 342
10.2. A Critique of the Governmental Internet Content Regulation 345
10.3. Is the Co-operative Model a Right Answer? 348
10.3.1. Risk of Self-Regulation 350
10.3.2. Limitation of International Consent 351
10.3.3. Defect of Technical Solutions 352
10.3.4. Recommendations 354
10.4. The Future of Internet Content Regulation 355

BIBLIOGRAPHY 363

APPENDIX A
Technical Specifications of Reviewed Filtering Software 407
APPENDIX B
Comparative Table: Technical Specifications of
Reviewed Filtering Software 418
APPENDIX C
Technical Review: 10 Examples of Commercial Filtering Software:
The List of the Sample Websites and the Detailed Results 420
APPENDIX D
The SafeSurf SS~~ Rating Standard 431
APPENDIX E
The Statistics of ICEC Deliberations (1997-2002) 436
APPENDIX F
Notification of the Commission on Youth Protection (No. 2000-31) 443
APPENDIX G
Questionnaire: The Impacts of the Internet Content Rating System
on the Actual Internet Contents in South Korea 445
APPENDIX H
The Questionnaire Sample List 453

List of Abbreviations

ARPA	Advanced Research Projects Agency
ACLU	American Civil Liberties Union
ALA	American Library Association
ABA	Australian Broadcasting Authority
CDA	Communication Decency Act, US
CDT	Center for Democracy and Technology
CERN	European Organization for Nuclear Research
COPA	Child Online Protection Act, US
CIPA	Children's Internet Protection Act, US
CRE	Commission for Racial Equality, UK
CSIRO	Commonwealth Scientific & Industrial Research Organisation, Australia
CYP	Commission on Youth Protection, South Korea
DARPA	Defense Advanced Research Projects Agency, US
EC	European Commission
EFF	Electronic Frontier Foundation, US
EFA	Electronic Frontiers Australia
ENC	Electronic Network Consortium, Japan
EPIC	Electronic Privacy Information Centre, US
EU	European Union
FCC	Federal Communications Commission, US
FBI	Federal Bureau of Investigation, US
GILC	Global Internet Liberty Campaign
ITC	Independent Television Commission, UK
ICEC	Information Communication Ethics Committee, South Korea
IGLHRC	International Gay and Lesbian Human Rights Commissions
ILGA	International Lesbian and Gay Association

IMF	International Monetary Fund
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IFEA	Internet Free Expression Alliance
INHOPE	Internet Hotline Providers in Europe
IPCA	Internet PC Culture Association, South Korea
ISPA UK	Internet Services Providers Association UK
IWF	Internet Watch Foundation
ITU	International Telecommunication Union
KBC	Korean Broadcasting Committee
KESA	Korea Entertainment System Industry Association
KGIA	Korea Game Industry Alliance
KIDC	Korea Internet Data Center
KMRB	Korea Media Rating Board
KNIC	Korea Network Information Center
LGAAD	Lesbian and Gay Alliance Against Discrimination, South Korea
LINX	London Internet exchange
MOCIE	Ministry of Commerce, Industry and Energy, South Korea
MCT	Ministry of Culture and Tourism, South Korea
MIC	Ministry of Information and Communication, South Korea
NCA	National Computerization Agency, South Korea
NLC	National Law Center for Children and Families, US
NLIP	Netherlands Internet Providers
NSF	National Science Foundation, US
OFLC	Office of Film and Literature Classification, Australia.
OECD	Organisation Economic Cooperation and Development
OPA 1959	Obscene Publications Act 1959, UK
RSACi	Recreational Software Advisory Council on the Internet
SRI	Stanford Research Institute

ICRA	The Internet Content Rating Association
UCLA	University of California Los Angeles
UCSB	University of California Santa Barbara
UTAH	University of Utah in Salt Lake City
NSF	National Science Foundation, US
W3C	World Wide Web Consortium
YMCA	Young Men's Christian Association
YWCA	Young Women's Christian Association

List of Tables

Table 4.1.	Filtering products	142
Table 4.2.	Filtering coverage	143
Table 4.3.	Filtering methods	145
Table 4.4.	Reporting	149
Table 4.5.	Usability	153
Table 4.6.	Filter list categories	156
Table 4.7.	A related term of each category	157
Table 4.8.	Number of blocked Websites	158
Table 4.9.	Over-blocked Websites by Norton Internet Security	160
Table 4.10.	Over-blocked Websites by We-Blocker	162
Table 5.1.	The syntax of the RSACi's label	186
Table 5.2.	PICSRules clauses	193
Table 5.3.	Description of the sample label	199
Table 5.4.	RSACi rating system descriptors	200
Table 5.5.	Usage of the RSACi and the ICRA systems among the top 19 sites	202
Table 5.6.	ICRA descriptors and associated codes	206
Table 5.7.	ICRA codes of the sample label	207
Table 5.8.	ICRAplus filtering test	210
Table 6.1.	The content rating system in South Korea	237
Table 7.1.	The SafeNet's rating standards	258
Table 7.2.	ICEC Recommendation list by age	258
Table 7.3.	The syntax of the harmful-to-youth material indication System	264
Table 7.4.	The statistics of ICEC deliberations	267
Table 7.5.	ICEC's deliberation categories and the number of deliberations in 2002	268

Table 8.1. The result of the questionnaire [Q4] 292
Table 8.2. The result of the questionnaire [Q5] 293
Table 8.3. The result of the questionnaire [Q5a] 294
Table 8.4. The result of the questionnaire [Q6] 295
Table 8.5. The result of the questionnaire [Q7] 296
Table 8.6. The result of the questionnaire [Q8] 297
Table 8.7. The result of the questionnaire [Q9] 298
Table 8.8. The result of the questionnaire [Q10] 299
Table 8.9. The result of the questionnaire [Q11] 300
Table 8.10. The result of the questionnaire [Q12] 300
Table 8.11. The result of the questionnaire [Q13] 301
Table 8.12. The result of the questionnaire [Q14] 303
Table 8.13. The result of the questionnaire [Q15] 304
Table 8.14. The result of the questionnaire [Q16] 305
Table 8.15. The result of the questionnaire [Q17] 305
Table 8.16. The result of the questionnaire [Q18] 307
Table 8.17. The result of the questionnaire [Q19] 308
Table 8.18. The result of the questionnaire [Q20] 309
Table 8.19. The result of the questionnaire [Q21] 309
Table 8.20. The result of the questionnaire [Q22] 310
Table 8.21. The result of the questionnaire [Q23] 311
Table 8.22. The result of the questionnaire [Q24] 311
Table 8.23. The result of the questionnaire [Q25] 312

List of Figures

Fig. 3.1.	A co-operative regulation model	123
Fig. 4.1.	Filtering at an end-user level	139
Fig. 4.2.	Filtering at a ISP level	140
Fig. 4.3.	Third-party filtering	141
Fig. 4.4.	Cyber Snoop's 'Time Controls'	147
Fig. 4.5.	Cyber Snoop's block list window	151
Fig. 4.6.	Net Nanny's block list window	152
Fig. 5.1.	Microsoft IE Content Advisor with the RSACi system	188
Fig. 5.2.	Third-party labelling	191
Fig. 5.3.	Layer cake model	204
Fig. 5.4.	The ICRA*filter*	209
Fig. 7.1.	Self-rating and third-party rating service of ICEC	259
Fig. 7.2.	The graphic logo of the harmful-to-youth material indication system	260
Fig. 7.3.	A sample Web page with the harmful-to-youth material indication system	261
Fig. 7.4.	Microsoft IE Content Advisor for the harmful-to-youth material indication system	263
Fig. 10.1.	A collective regulatory model	356

CHAPTER 1
INTRODUCING THE INTERNET

1.1. Introduction

It is said that we are living, at the beginning of the 21st century, in the so-called "Internet era." (Ramadorai, 2000) For the last decade, this phenomenal new medium has been integrated into our daily lives at breakneck speed. Every day, we use it not only for private communications, but also for mass public communications. Through the Internet, millions of people exchange mail and have chats with their friends or even with strangers from thousands of miles away. Millions of people also read the newspapers, listen to radios and have access to libraries on the Internet. Others buy and sell all kinds of goods over the Internet. Indeed, many enjoy the great benefits from this revolutionary global medium. The Internet provides a relatively cheap, easily accessible and strongly interactive environment for the global circulation of a vast amount of information. In this sense, it is argued that the Internet represents, "a fundamental enhancement of human freedom, with a transforming potential that is worth defending" (Brin, 1997, p. 32), which has great potential to give, "one person the power to reach another person or a million people equally easily." (Bennahum, 1996, p. 45) Moreover, it is referred to as, "the most participatory form of mass speech yet developed." (*ACLU v. Reno* 929 F. Supp. 824, 1996) People often metaphorically call this new medium 'the information superhighway.'

However, just like real highways, this superhighway is not a place where all drivers are people of goodwill. Just as some people carry illegal goods, for instance contraband cigarettes or prohibited drugs, on a highway, it is also evident that a small number of people use the information superhighway for rather unpleasant or even criminal purposes. A small segment of information on the Internet, such as child pornography, is illegal in most countries worldwide. Some other information which is available on the Internet, such as explicit

sexual information and extreme political propaganda, is considered offensive or inappropriate by certain people for various reasons, ranging from political reasons to religious and cultural grounds. Since the use of the Internet started to explode in the mid-1990s, the easy and wide availability of illegal and harmful content on the Internet has been a great concern to governments and individuals throughout the world. Many governments, from the US and Australia to China, have taken action on these issues in various ways (see Chapter 2.6), while at the same time there have been strong counter-movements to protect the Internet against governmental interventions and to preserve its independent nature (see Chapters 1.4 & 2.3). My arguments start at this point. Should the Internet be regulated? If so, how it can be effectively regulated? Who can control it? What is the best solution for these issues? In this context, this thesis aims to explore the issues relating to content regulation and freedom of expression on the Internet with reference to South Korea.[1]

My main case study is the South Korean government's Internet content rating system and Internet content regulation. South Korea is an interesting case, because it established an extensive Internet infrastructure and become the first country in the world which to adopt the broadband Internet connection nationwide (see Chapter 6). While the South Korean government has successfully pursued policies intended to make it a leader in terms of Internet usage, its Internet content policy has been criticised for excessively restricting freedom of expression on the Internet by a number of civil organisations, such as the JINBO Network Centre (see Chapter 7). Notably, it introduced the world's first mandatory Internet content rating system. This thesis will study issues in

[1] In this thesis all Korean terms are romanized according to the official Korean language romanization system which was released by the South Korean government in 2000. The official instruction of the Romanization of Korean (Ministry of Culture and Tourism proclamation No. 2000-8) is available in English at http://english.tour2korea.com/02Culture/KoreanLanguage/roman_korean_language.asp (Retrieved May 3, 2005).

depth related to the government-centred Internet content regulation and the mandatory rating system in South Korea.

Academic debate over Internet content regulation in South Korea began in around 1996. Professor Hwang Sang-Jae's article in *HANGUK EONRON HAKBO* [*Journal of Journalism and Communication Studies*], MINJUJEOK COMMUNICATION GONGGANEURO CYBERSPACEUI GANEUNGSEONGGWA HANGYE [A Feasibility and limitation of cyberspace as a sphere for democratic communication] (S. J. Hwang, 1996), is one of the earliest Korean works which deal with issues of freedom of expression and regulation on the Internet. Since then, discussions about these issues have been developed mainly by three distinctive groups: jurisprudence academics, communication studies academics and governmental research agencies, such as HANGUK JEONSANWON [Korean National Computerization Agency] and JEONGBO TONGSIN JEONGCHAEK YEONGUWON [Korea Information Strategy Development Institute].

For the study I consulted a number of the Korean literature, including *JEONGBO GWAHAK HEOJI* [*Journal of Information Sciences*], *JEONJA TONGSIN DONGHYANG BUNSEOK* [*Analysis of Electronic Communication Trend*], *COMMUNICATIONHAK YEONGU* [*Journal of Communications studies*], *CYBER COMMUNICATION HAKBO* [*Journal of Cyber Communications Studies*], *JEONGBOHWA JEONGCHAEK* [*Journal of Information Policy Studies*], *JEONGBO TONGSIN JEONGCHAEK* [*Journal of Information and Communications Policy*], *INTERNET BEOPRYUL* [*Journal of Internet law*], and other Korean law journals — but I found that the first two journals are not relevant to this thesis, because they largely focus on issues of telecommunication engineering. Furthermore, a number of reports and documents from governmental agencies and non-governmental organisations were also consulted, such as JEONGBO TONGSIN YUNRI WIWONHOE [Information and Communication Ethics Committee] and the

JINBO Network Centre.

Alongside this case study, the thesis gives attention to the EU's co-regulatory scheme, the 'Action Plan on Promoting Safer Use of the Internet' which forms a significant contrast to the government-centred Internet content regulation in South Korea. The Action Plan incorporates the following action lines; creating *a network of hotlines*, encouraging *self-regulation*, developing *filtering and rating systems* and encouraging *awareness campaigns*. Taking into account the global and interactive characteristics of the Internet, it is significant that the EU adopted a co-regulatory model, while other governments, including the US, hurried to introduce legal regulation to control content on the Internet. The EU Action Plan will be discussed in Chapter 2 and 3 and it will be referred to throughout the thesis.

Before the case study of South Korea, the thesis considers the issues of free speech rights on the Internet, governmental Internet content regulation, self/co-regulation of Internet content and filtering/rating systems respectively from Chapter 2 to 5. Here, the thesis begins with preliminary discussions about the history of the Internet and its distinctive nature.

1.2. The Emergence of the Internet

Before discussing any Internet-related issue, it is an essential prerequisite to understand the characteristics of the Internet which significantly differ from the classic attributes of other existing media. In order to understand the Internet's unique features, I shall briefly discuss the early history of the Internet to examine how its distinctive attributes and technical architectures have been developed.

In the beginning the Internet was merely one of many new communication technologies designed for a limited number of experts. Ironically, this anarchic medium originated from a military research network developed by the Advanced Research Projects Agency (ARPA),[2] the so-called ARPANET. In the early 1960s with the support of the US Air Force the RAND Corporation, a US policy think-tank, studied a concept of packet-switching[3] networks which have no central controlling body and could therefore withstand a nuclear attack. A series of its reports, entitled *On Distributed Communications*, was finally published in 1964. Paul Baran (1964), a main author of the reports, introduced "a communication network which [would] allow several hundred major communications stations to talk with one another after an enemy attack," and outlined "the requirements for and design consideration of the distributed digital data communications network" in special reference to "the use of redundancy as a means of withstanding heavy enemy attacks." On this principle a UK institution, the National Physical Laboratory, set up the first test network in 1968 (Hardy, 1993; Sterling, 1993). In December 1969, the first

---

[2] ARPA was established under the US Department of Defense, in February 1958, in response to the Soviet Union's launch of the first successful artificial satellite, Sputnik, in 1957. It was renamed the Defense Advanced Research Projects Agency (DARPA) in 1972.

[3] According to the *Penguin Concise Dictionary of Computing* (Pountain, 2003, p. 318), 'packet-switching' can be defined as follows:

> An important communication technique in which messages are decomposed into many small portions called PACKETS, which are then individually transmitted to the destination following a route determined by a ROUTING algorithm.

Sterling (1993) described its mechanism as follows:

> [On the network] the messages themselves would be divided into packets, each packet separately addressed. Each packet would begin at some specified source node, and end at some other specified destination node. Each packet would wind its way through the network on an individual basis. The particular route that the packet took would be unimportant. Only final results would count. Basically, the packet would be tossed like a hot potato from node to node to node, more or less in the direction of its destination, until it ended up in the proper place. If big pieces of the network had been blown away, that simply wouldn't matter; the packets would still stay airborne, lateralled wildly across the field by whatever nodes happened to survive.

online demonstration of the ARPANET linked four nodes; the University of California Los Angeles (UCLA), the University of California Santa Barbara (UCSB), the University of Utah in Salt Lake City (UTAH) and the Stanford Research Institute (SRI) via 50K bps (bits per second) circuits (Hauben, 1993). Thereupon, a project – which was supported by one of the most hierarchical organisations; the military – contradictorily conceived one of the most decentralised and even anarchic medium we have ever known. This new network's liberal features started to appear in less than a year after it was launched.

> ARPANET's users have warped the computer-sharing network into a dedicated, high-speed, federally subsidised electronic post-office. The main traffic on ARPANET was not long-distance computing. Instead, it was news and personal messages. [...] One of the first really big mailing-lists was "SF-LOVERS," for science fiction fans. Discussing science fiction on the network was not work-related and was frowned upon by many ARPANET computer administrators, but this didn't stop it from happening (Sterling, 1993).

Indeed, people were using the ARPANET not only for their work but also for very personal purposes. They soon became far more passionate about e-mailing than they were about long-distance computing. In the 1970s most Internet users were academics and engineers, since network environments, which required expertise and expensive equipment, were not easily accessible to the public. There were only 37 nodes in the ARPANET by 1972 (Sterling, 1993). "In 1981 fewer than 300 computers were linked to the Internet [worldwide]." (*ACLU v. Reno* 929 F. Supp. 824, 1996, Findings of Fact [3]) This new electronic network was growing steadily, but quite slowly. In 1983 ARPANET's military segment broke off and became MILNET and its original transmission protocol, Network Control Protocol (NCP) was replaced with TCP/IP (Transmission Control Protocol / Internet Protocol) which became a core standard protocol of

the modern Internet. From the mid-1980s the growth of the Internet accelerated. In 1986 the National Science Foundation (NSF), a US governmental agency which was established in 1950, funded a backbone network which directly connected its super-computer centres at 56K bps. Two years later its backbone network, which was dubbed NSFNET, was upgraded to 1.544M bps. In 1990, the NSFNET took over ARPANET's role as network backbone and the ARPANET formally expired (Hardy, 1993; Zakon, 2004). In the early 1990s the Internet finally reached a crucial turning point. The NSF lifted restrictions on the commercial use of the Internet in 1991,[4] and the World Wide Web and the first widely-distributed graphical browser, Mosaic,[5] were released in 1992 and in 1993 respectively. The Internet population has skyrocketed.

Since then, the Internet has rapidly grown into a global medium. Now it has become something that has its own vitality. The Internet has enabled people to create their own virtual spaces and even communities worldwide. Everyday, hundreds of millions of "netizens" post enormous amounts of information on the Web and participate in these virtual communities according to their interests and needs, ranging from academic and political communities to online game communities. Gregory Gromov, the author of *Roads and Crossroads of Internet History*, said, "We can't imagine yet the real scale of the recent shake, because there have not been so fast growing multi-dimension social-economic processes in human history." (Gromov, 1995) Indeed, the Internet has

---

[4] Since then, US Pizza Hut first offered pizza ordering on its Website in 1994. In 1995 the registration of domain names stopped being free, because the NSF prohibited direct access to its backbone and contracted with commercial companies which would be providers of access to the backbone. Traditional on-line dial-up system, such as Compuserve, American Online and Prodigy, began to provide Internet access. Since then, thousands of shopping malls and banks have emerged on the Internet. Commercialisation of the Internet has been accelerated.

[5] Mosaic was developed by Marc Andreesen in 1992. He was a student and part-time assistant at the National Center for Supercomputing Applications (NCSA) at the University of Illinois, US.

profoundly changed how people work, study, play and communicate during the last decade. The widespread use of broadband Internet services is accelerating these changes even faster. It is not too much to say that the all-pervasive influence of the Internet amounts to a social revolution.

1.3. The Nature of the Internet

How has the Internet led these revolutionary changes? What makes the Internet such a significant worldwide communication medium? To answer these questions, it is now necessary to consider the unique characteristics of the Internet. As already outlined, the first significant characteristic of the Internet is decentralisation. Poster (1997, p.204) discussed that:

> The Internet is above all a decentralised communication system. [...] The Internet is also decentralised at a basic level of organisation since, as a network of networks, new networks may be added so long as they conform to certain communications protocols.

Indeed, it is a network of networks based on various technologies and socio-cultural backgrounds worldwide. Each network has an independent infrastructure. However, it is interconnected with countless other networks by communications protocols, such as the File Transfer Protocol (FTP) and the Hyper Text Transfer Protocol (HTTP). Through the *ACLU v. Reno* case the US court stated as follows:

> The Internet is [...] a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. [...] Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organisations, and some are privately owned. The resulting whole is a decentralised, global medium of communications [...] that links people, institutions,

> corporations, and governments around the world (*ACLU v. Reno* 929 F. Supp. 824, 1996, Findings of Fact [1]—[4]).

Various parties worldwide, ranging from governments to commercial companies, have participated in building the Internet. Some media, such as television and the telephone, are controlled by centralised authorities within national boundaries. However, there is no central controlling body for the Internet. Therefore, no single government can control the entire Internet. In this context, Wallace and Mangan (1997b, p. xiv) said, "The Internet is a forum without gatekeepers." Thornburgh and Lin (2002, p. 33) even argued, "[T]he basic design philosophy underlying the Internet has been to push management decisions to as decentralised a level as possible."

Secondly, the Internet has fundamentally changed our spatial notions, since communication and information through the Internet know no geographical borders and spread all over the world at once. Former US Vice President, Al Gore stated:

> [...] we now have at hand the technological breakthroughs and economic means to bring all the communities in the world together. We now can at last create a planetary information network that transmits messages and images with the speed of light from the largest city to the smallest village on every continent (Schiller, 1996, p. 91).

On the Internet it is common practice that peoples' activities take place outside their own government's jurisdiction. For instance, any Internet user is able to get across the Atlantic Ocean in a second, from a UK museum Website to a Canadian university site, simply by typing a URL (Uniform Resource Locator) on his or her Web browser. Moreover, some domain names, such as '.com', '.net' and '.biz', do not indicate their nationalities. In this context, Stefik (1999, p. 251) argued that the Internet might challenge territorial identity as follows:

> The Net [...] unsettles and challenges our distinctions about identity. It runs right across national borders – challenging the control that countries exercise at their borders. It connects people of different social groups. By obliterating boundaries that have limited people's interaction in the past, the Net has the potential to destabilise some of our collective ideas about self and other.

Consequently, the traditional concept of territory has faced a serious challenge from the Internet, which has a global audience, which can easily cut across territorial borders. According to the Britannica Encyclopedia ("Territory," 2002), a general definition of territory is "a geographical area belonging to or under the jurisdiction of a governmental authority," but the definition can be more diverse depending on the various situations that are given. For instance, a house can be an independent territory. Also, the room where anyone is staying at the moment can be a territory. Almost all geographical spaces – ranging from a school to a country or continent or even the universe – all can be defined as a territory. However, for this study I shall interpret the definition of territory as an extent of land under the jurisdiction of a sovereign nation. Johnson and Post (1996) argued that the Internet would threaten territorial-based regulation systems in their article, *Law and Borders*, as follows:

> Global computer-based communication cut across territorial borders, creating a new realm of human activity and undermining the feasibility – and legitimacy – of applying laws based on geographic boundaries. While these electronic communications play havoc with geographic boundaries, a new boundary, made up of the screens and passwords that separate the virtual world from the "real world" of atoms, emerges. [...] Territorially-based law-making and law-enforcing authorities find this new environment deeply threatening.

John Perry Barlow (1996a), a co-founder of the Electronic Frontier Foundation

(EFF)[6], claimed that the borderless and uncontrollable Internet calls into question the very idea of a nation-state. Newey (1999) said that some might claim that the Internet could put an end to national legal systems, because of the given Internet environment which is international by its very nature. He admitted, however, such claims might be implausible, but pointed out, "they do at least point up the severity of the legal questions that the Internet is raising." (p.17)

In fact, the turmoil of territory on the Internet has influenced various issues, both political to cultural. Authoritarian countries have treated the Internet as an acute threat to their sovereignty, because the Internet provides and distributes a vast amount of information that can be dangerous to their social order regardless of any geographical borders. Indeed, "geographical proximity and content availability are independent of each other" on the Internet, "since a document can as easily be retrieved from a server 5,000 miles away as one five miles away." (Boyle, 1997)

Certain information can be illegal material in some countries, but it can be legal material in other countries. In the case of a country which is organised on a federal basis, the problem becomes more complex.[7] These kinds of problems

---

[6] In July 1990, the Electronic Frontier Foundation (EFF) was founded in response to the Steve Jackson Games case, which raised the issue of free speech and privacy rights in cyberspace. Inspired by this case, Mitch Kapor, former president of Lotus Development Corporation, John Gilmore, an early employee of Sun Microsystems, and John Perry Barlow, who were members of electronic community called the Whole Earth 'Lectronic Link' (now WELL.com) formed EFF to work on civil liberties issues raised by new technologies. (Resource: EFF Website: http://www.eff.org/about. Retrieved May 1, 2003)

[7] For instance, in the US each state has different state laws. Lessig (1999, pp. 54-55) takes Internet gambling as an example. Minnesota has a strong state policy against gambling. It is a misdemeanour, unless it has done "pursuant to an exempted or state-regulated activity, such as licensed charitable gambling or state lottery," while most other states in the US allow their citizens to gamble.

have often resulted in a dispute concerning jurisdiction. Consider this case: someone posts an illegal Web page using a domestic server. The police or Internet service may close down the site. However, if someone still has the will to reopen the site and has not been arrested yet, s/he can easily reopen it as if it were located abroad even though it is actually located at his or her home. Expanding the case, if s/he goes abroad where her or his site is legally treated under different legal guidelines and reopens the site there, the site will be continuously accessible worldwide including in her or his home country and s/he will never be prosecuted or arrested. For instance, while neo-Nazi propaganda is illegal in Germany and the Netherlands, it is constitutionally protected in the US. Ernst Zűndel's Website is a prime example.

> A good real-world illustration of the difficulties is provided by the Website operated by the well-known Holocaust denier, Ernst Zűndel. The Zűndelsite, as it is known, is housed in California, but it is evident that some of the material it contains is illegal under German laws which ban any denial of the historical truth of the Holocaust and the dissemination of Nazi propaganda. It has provided impossible to bring charges under German law against Zűndel and his colleagues, since they are working within a separate jurisdiction where the material they are providing is legal (Newey, 1999, p. 19).

Thirdly, the Internet is incredibly interactive. It is based on a very different communications model from the other media. In the traditional media, such as newspapers and broadcasting, there is a strict division between providers and recipients. The fundamental rule regarding the old media is that only providers transmit opinions or information to recipients and the content is always decided by the providers. Recipients are in a passive position. For instance, audience participation in TV programmes is extremely limited.[8] However, Internet users

[8] The emergence of digital interactive TV is now changing the nature of TV. Unlike analogue TV, people can select schedules or take part in games as a contestant through digital TV. It even provides broadband access to the Internet. Although digital TV has not been available for long

can react immediately to information found on the Internet. The difference between providers and recipients is not clear cut on the Internet which provides truly bi-directional communication. In principle, all Internet users can be suppliers of contents and not merely recipients, since the Internet allows various interactive communication from one to one, from one to many, from many to one, and from many to many.[9] Furthermore, "The capital costs of becoming an Internet publisher are relatively low, and thus anyone can establish a global Web presence at the cost of a few hundred [pounds]." (Thornburgh & Lin, 2002, p. 35) Thus these attributes of the Internet have resulted in the free flow of information all over the world and eventually led the so-called Internet revolution.

1.4. The Literature on Internet Regulation: A Utopian Vision and a Digital Panopticon

The emergence of the Internet era is viewed in a variety of perspective. On the one hand, a utopian vision claims that the Internet is fundamentally free. This view has been built up by Internet enthusiasts who experienced the early Internet cultures which were built on "norms of collaboration and cooperation." (Rheingold, 2000, p. 364) It considers the advent of the Internet

---

in the UK, it is proving to be very popular. According to a report, "Either by cable, satellite or Freeview, 53 per cent of UK households have at least one digitally enabled television." (Malone, 2004) The issue of digital TV is not covered by this thesis.

[9] In 1996 the US court of *ACLU v. Reno* defined the most common methods of communication on the Internet as six categories in its Findings of Fact (22) as follows (*ACLU v. Reno* 929 F. Supp. 824, 1996):

1. One-to-one messaging (such as "e-mail"),
2. One-to-many messaging (such as "listserv"),
3. Distributed message databases (such as "USENET newsgroups"),
4. Real time communication (such as "Internet Relay Chat"),
5. Real time remote computer utilisation (such as "telnet"), and
6. Remote information retrieval (such as "ftp, " "gopher, " and the "World Wide Web").

as a revitalisation of the public sphere[10] and grass-roots democracy. Mitchell (1995) and Rheingold (2000) argued that the Internet could be a digital agora in the 21st century. Dertouzos (1997, p. 9) described the Internet as the Athens flea market as follows:

> Almost all of the people were friendly and talkative, tackling every conceivable topic between deals. They formed a community that stretched beyond its commercial underpinnings. There was no central authority anywhere; all the participants controlled their own pursuits. It seemed natural and inevitable to me that the future world of computers and networks would be just like the Athens flea market – only instead of physical goods, the commodities would be information goods.

John Barlow (1996b) even argued for unlimited freedom of expression and objects to any legal restrictions on the Internet through his famous manifesto, *A Declaration of the Independence of Cyberspace*. He claimed that the Internet is naturally independent of any governmental regulation and stated, "We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge." Barlow's utopian vision has strongly influenced numerous Internet enthusiasts. Newey (1999, p. 16-17) claimed, "The nature of the Internet itself is resistant to content regulation." John Gilmore stated, "The Net interprets censorship as damage and routes around it." (Reagle, 1999) Slevin (2000, p. 214) explained that these opinions are based on "what they see as the anti-authoritarian and liberating nature of the Internet." He also argues that these opinions claim, "Efforts to regulate the Internet [...] are destined to

---

[10] Public sphere means "a domain of our social life in which such a thing as public opinion can be formed." (Habermas & Seidman, 1989, p. 231) This concept of public sphere is developed by Jürgen Habermas. He wrote;

> Access to the public sphere is open in principle to all citizens. [...] Citizens act as a public when they deal with matters of general interest without being subject to coercion; thus with the guarantee that they may assemble and unite freely, and express and publicise their opinions freely. (Habermas & Seidman 1989, p. 231)

flounder because cyberspace is inherently global and pliant, allowing individuals and organisations to evade authorities by slipping into anonymity and by retreating beyond the bounds of their jurisdictions." Indeed, as Sunstein (2001, p. 136) said, these utopian visions strongly resist government regulation and endorse "laissez faire" and "voluntary norms founded in enlightened self-interest."

Contrary to this, a gloomy view counts the Internet as a digital "Panopticon."[11] (S. O. Hong, 2002, p. 73-103) This opinion strongly rejects the utopian vision and takes a pessimistic view of the future of the information society. A science-fiction writer, Vernor Vinge said, "The future would be a world of perfect regulation, and the architecture of distributed computing – the Internet and its attachments – would make that perfection possible." (Lessig, 1999, p. ix) In other words, although the Internet frees us from physical limitations of

---

[11] The Panopticon was proposed as a model prison by Jeremy Bentham (Philosopher and social reformer, 1748-1832).

> [It] incorporates a tower central to an annular building that is divided into cells, each cell extending the entire thickness of the building to allow inner and outer windows. The occupants of the cells [...] are thus backlit, isolated from one another by walls, and subject to scrutiny both collectively and individually by an observer in the tower who remains unseen (Barton & Barton, 1993, p. 139).

Bentham's central goal of the panopticon was "control through both isolation and the possibility of constant surveillance." Engberg (1996) discussed that Bentham found "this Utilitarian ideal of oppressive self-regulation to be appealing in many other social settings, including schools, hospitals, and poor houses." Foucault (1975/1977) applied it as a metaphor for the oppressive use of information in a modern disciplinary society in his book, *Discipline and Punish.* According to him, modern society is organised "like so many cages, so many small theatres, in which each actor is alone, perfectly individualised and constantly visible." (p. 200) He argues that:

> [The Panopticon] makes it possible to perfect the exercise of power. [...] Because it is possible to intervene at any moment and because the constant pressure acts even before the offence, mistakes or crimes have been committed. Because, [...] its strength is that it never intervenes, it is exercised spontaneously and without noise, it constitutes a mechanism whose effects follow from one another. Because, without any physical instrument other than architecture and geometry, it acts directly on individuals; it gives 'power of mind over mind.'" (p. 206)

traditional media, it gives authorities greater opportunities to monitor and record our every single online activity. Lessig (1999, p. 5) argued in his book, *Code and other Laws of Cyberspace*, as follows:

> The word [cyberspace] itself speaks not of freedom but control. Its etymology reaches beyond a novel by William Gibson (Neuromancer, published in 1984) to the world of "cybernetics", the study of control at a distance.

Lessig rejects the idea that cyberspace cannot be controlled by governments, but claims the Internet architectures have been born from the very idea of control. As a constitutionalist he believes, "Liberty in cyberspace will not come from the absence of the state, [but it] will come from a state of a certain kind." (Lessig, 1999, pp. 3-8) Ithiel de Sola Pool (1983, p.3) also claimed that deregulation cannot protect freedom of speech and stated, "Deregulation, whatever its economic merits, is something much less than the First Amendment."

Lessig (1998) argued in his article, *The Law of Cyberspace*, "Just as in real space, behaviour in cyberspace is regulated by four sorts of constraints" as follows: law, norms in cyberspace, the market and code. Firstly, many kinds of the laws, such as copyright law, defamation law, or sexual harassment law, constrain cyberspace. Secondly, norms in cyberspace govern behaviour and expose individuals to sanction from others. Thirdly, the market coerces cyberspace, for instance, through changing the price of access. Fourthly, Lessig emphasised the importance of code which constitutes cyberspace:

> This code, like architecture in real space, sets the terms upon which I enter, or exist in cyberspace. It, like architecture, is not optional. [...] life in cyberspace is subject to the code, just as life in real space is subject to the architectures of real space.

Indeed, the Internet has never been free from certain forms of constraint. Moreover, as Slevin (2000) argued, it has always been scrutinised by nation-states. The history of the Internet itself proves this. As discussed above, it originated as part of a US military research network and a US governmental agency, the NSF, played a decisive role in developing its initial infrastructure. The body which lifted restrictions on the commercial use of the Internet was also the NSF. The Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for the domain name system management, has been criticised for its close relationship with the US Department of Commerce (Akdeniz, Walker & Wall, 2000, p. 10). It cannot be denied that the early Internet had been developed under the US government's primary influence and enormous subsidies, although I believe that the most important impetus of the Internet's significant growth has been the spontaneous participation of Internet users.

Another criticism against the above utopian vision has been made by Barbrook and Cameron (1995). They defined this utopian vision, so-called "Californian Ideology," as an odd mix of cybernetics, free market economics and counter-culture libertarianism:

> The Californian Ideology offers a fatalistic vision of the natural and inevitable triumph of the hi-tech free market – a vision which is blind to racism, poverty and environmental degradation and which has no time to debate alternatives.

Barbrook (1996, pp. 56-58) argued in his article, *HyperMedia Freedom*, "The electronic agora is yet built," and these utopian visions are "trying to avoid facing the political and economic contradictions of really existing capitalism." From a worldwide point of view Castells (2004) criticised the electronic agora for neglecting the fact that large numbers of the global population, mainly from

many undeveloped nations, are still being excluded from all the benefits of the Internet:

> That is, while a relatively small, educated, and affluent elite in a few countries and cities would have access to an extraordinary tool of information and political participation, actually enhancing citizenship, the uneducated, switched-off masses of the world, and of the country, would remain excluded from the new democratic core, as were slaves and barbarians at the outset of democracy in classical Greece (p. 416).[12]

As Loader (1998, p.9) argued, the information-poor are an extensive social phenomenon. They are excluded from opportunities to utilise the Internet, because of race, disability, class, location or religion. Haywood (1998) argued that the Internet has not been able to change social divisions and distinctions very much. Therefore, there is a huge gap between the information-rich and the information-poor on the Internet. Schiller (1996, p. xi) pointed out, "Inequality of access and impoverished content of information are deepening the already pervasive national social crisis" in the US where the Internet was incubated. In my view, Internet visionaries' optimistic anticipation is an empty dream from the viewpoint of the information-poor. Resisting governmental regulation and endorsing laissez faire cannot be a solution for problems of digital divide on the Internet. On the contrary, a government may play a decisive role in developing the Internet. For instance, in terms of public policy the South Korean government has strongly promoted Internet usage and established an extensive Internet infrastructure (see Chapter 6) — the issue of inequality on the Internet is another important area of study but it is not covered by this thesis.

---

[12] During the 1970s and the 1980s, most Internet users were "relatively small, educated, and affluent" elites as Castells argued above. However, over the last few years the numbers of Internet users in many developed nations have significantly increased. In 17 countries including the UK, the US, Canada, Australia and Japan, the ratios of Internet users have already reached over 50 percent of their whole population as of 2003 (KRNIC, 2003).

Alongside issues of information inequality, the pessimistic view claims that there is a latent danger that the Internet could work as Orwell's Big Brother in the 21st century. Technically, this digital network is able to collect our personal data and to monitor our every activity on it without our acknowledgment or consent — the issue of privacy on the Internet is also a significant field of study which is not covered by the thesis. Raab (1997, pp. 155-156) said that:

> [...] applications of information and communications technologies (ICTs) might promote government, commerce and democracy but also hold the threat of increasing surveillance over persons and groups, thus raising the spectre of 'Orwell' in the midst of the realisation of 'Athenian' ideas.

However, this does not necessarily mean that the Internet is totally under surveillance or that it is a threat to civil liberties. As Kranzberg (1985, p. 50) stated, "Technology is neither good nor bad, nor is it neutral." Castells (2001, p. 171) also argued, "The Internet is no longer a free realm, but neither has it fulfilled the Orwellian prophecy." In my view, the Internet is neither a utopian medium nor a tool for tyranny, but it gives us greater opportunities and dangers together.

For the last decade the Internet has gained massive popularity and has became one of the most important communication and information media in modern society. Behind its significant successes, however, a dark side has also grown. Just like in the real world, a variety of dangers, from copyright disputes to privacy issues, exist on the Internet. Although these problems are not limited to the Internet, as discussed above, because of the characteristics of the Internet, such as globalisation, anonymity, synchronisation, and strong interactivity, the problems are more complicated than the equivalent problems in the real world. Indeed, as Castells (2001, p. 171) said, "It is a contested terrain, where the new, fundamental battle for freedom in the information age is being fought."

1.5. Regulating Information on the Internet

Ironically, from Gutenberg's press to the advent of cable television, sex and pornography have played an important role in winning the popularity of new communication technologies. Tierney (1994) wrote in his article, *Porn, the low-slung engine of progress*, as follows:

> When Gutenberg's press brought the written word to the masses in the late 1400's, it didn't take long for printers to discover that the masses wanted more than Bibles. A book of erotic engravings depicting lovemaking positions, published in 1542 [...] Some of the earliest daguerreotypes,[13] in the mid-1800s, were pornographic. One of the first movies, made by Thomas Edison, was a bit of realism called, "The Kiss", and a pornographic film industry was thriving by the 1920s [...] They played a key role in popularising the videocassette recorder [in the late 1970s].

Akdeniz argues that this is "one of the major reasons why each new communications medium promptly triggers cries for censorship." (Akdeniz & Strossen, 2000, p. 207) Indeed, the Internet medium has brought up the very same question. As mentioned above, the Internet has offered, "a 'brave new world' in the most positive sense, in that it is the most powerful communication tool in history." (Dixon, 2002, p. 39) At the same time, however, it is considered to have dangerous elements, since it has been used for objectionable or illegitimate purposes.

Whereas, as discussed above, some Internet visionaries refuse "government regulation or intervention as an aid to this process, and believe instead in the force of free markets and competition," (Grossman, 1997, p. 161) it is also

---

[13] Daguerreotype is a mid-19th Century form of photography invented by Louis Daguerre of France. The first daguerreotype image was produced in 1837 ("Photography: The pioneers," 2002).

argued that the importance or role of government in shaping the Internet cannot be dismissed (Bennahum, 1996). Lim (2003) emphasised the necessity of regulation on the Internet as follows:

> Regulation is necessary in cyberspace as without it, [...] the cyberworld will be subsumed in uncertainty and become rampant with abuse. [...] Unregulated, cyberspace is a brutal environment, where users' rights are virtually non-existent and the remedies are confused and uncertain. An unregulated cyberspace has the capacity to undermine entire legal systems, tear at community values and stifle commercial activity.

Dixon (2002, p.42) argued that without regulation people will lose the benefits of the Internet and free speech rights will not be protected:

> [If any effective regulation does not work,] the Internet will come to be viewed as some kind of anarchic Wild West and may people will be put off using it or allowing their children to use it. This in turn will deprive them of the many benefits of the Internet for education, entertainment, business and communication and for the younger generation in particular could well leave them disadvantaged in school and in the workplace. Free speech and access to it will in fact be restricted, not protected.

For these reasons, many governments worldwide have attempted to regulate the Internet in various ways. Among the many issues which are related to the Internet, freedom of expression has been one of the most important. In particular, the distribution of child pornography and propaganda for racial hatred through the Internet have been great concerns. In order to address these issues, a number of technical solutions, such as Internet content filtering software and the Internet content rating system have been developed (see Chapters 4 & 5). Some alternative regulatory proposals to direct governmental regulation have also been introduced (see Chapter 3.5). Regardless of whether we agree or disagree with the notion that the Internet should be regulated, in

reality it has long been subject to certain regulatory frameworks, ranging from direct governmental intervention to the Internet industry's self-regulation. However, Internet content regulatory attempts in many countries have not been entirely successful. They have experienced difficulties in achieving their regulatory goals and have been a target of severe criticisms (see Chapter 2.6). As Slevin (2000, p. 217) said, "There remains, in most countries of the world, great uncertainty about how states can best regulate the Internet in the interests of their citizens."

Milne (2002)[14] critically appraised the five main arguments against Internet content regulation; that it is infeasible, repressive, unnecessary, already solved and too expensive. The first argument is that it is *infeasible* to control what appears on the Internet, even if one wanted to, because it is an enormous global medium which is not grounded on a single geographical jurisdiction. However, it is argued that controlling Internet content is not an easy task, but this does not necessarily mean that it is an impossible mission. Darlington (2004)[15] claimed, "This is not an argument as to why regulation is undesirable but one as to why it is difficult and the fact that something is difficult does not mean that it should not be done." In reality, since the mid-1990s, many nations have taken actions on illegal content on the Internet, in particular child pornography. Many efforts to address these issues have been made at a supra-national level. For instance, Operation Hamlet in 2002 which cracked down on an international online child pornography network (see Chapter 3.6.2), and the European Union's 'Action Plan on Promoting Safer Use of the Internet' are prime examples (see Chapters 2.6.4.2 & 3.5).

---

[14] Claire Milne is an independent telecoms policy consultant and is a Board Member of the Internet Watch Foundation (IWF).

[15] Roger Darlington is the chair of the Internet Watch Foundation (IWF).

The second argument is based on a notion that freedom of expression would be *repressed* by any Internet content regulation. In principle, this argument is also correct — in many countries heavy-handed governmental Internet content regulation has had serious chilling effects on the Internet. The South Korean government's Internet content regulation, which introduced a mandatory Internet content rating system, is a prime example (see Chapters 7 & 8). This argument is not limited to the Internet, but is related to all information and communication media. However, this argument misses an important fact; that freedom of expression is not an absolute right. It is restricted for a variety of reasons, such as defamation, incitement to racial hatred, copyright infringement and so on. This issue will be discussed in depth in Chapter 2.

The third argument is that Internet content regulation is *unnecessary*, because the dangers of certain Internet content are exaggerated, and no real or serious problem with Internet content exists. Milne (2002) argued that this argument is dependant on what constitutes a 'real' and 'serious' problem. With certain Internet content some may feel uncomfortable or even offended, but some others may not. This is "always a matter of judgment."

The fourth contention is that technical solutions, such as Internet content filtering and rating systems, provide effective ways to address problems concerning Internet content, thus these issues are *already* almost *solved*. This argument is highly debatable. On the one hand, these technical solutions have been chosen as a feasible solution for protecting minors from inappropriate information on the Internet by many proponents, including parents, teachers and governments. On the other hand, these have been criticised for being a censorship tool which has inherent technical weaknesses. I will examine issues over these technical solutions in depth in Chapters 4 and 5 through case studies and technical reviews.

The final point is that the cost of Internet content regulation is *too expensive*. This argument was once valid when the Internet industry was fledgling and uncertain. Milne (2002) claimed, "Costs of regulation are not usually very great compared with many other costs of running a business." In many Western countries, the Internet industry has played a major role in Internet content regulation. This issue will be discussed further in Chapter 3.

The argument for legitimacy of Internet content regulation is a reverse of the argument we discussed above. Darlington (2004) argued that Internet content should be regulated for the following reasons. He firstly claimed that *the Internet is now open to every body*. "The Internet has users in every country in every group." In this sense, we need "some procedures for tackling illegal content on the Internet" and "some mechanism for allowing end user control of what is accessed on the Internet." The second ground is that *the Internet is no different from other electronic networks*. Darlington argued that the Internet is not "fundamentally different from other electronic communications networks," such as radio and television, which have been subject to regulation. The third argument is that *there is harmful content on the Internet.* Darlington said that on the Internet child pornography does exist in volume, although it may be a tiny proportion of the total Internet content and in most cases, "the production of this material has involved child abuse." His fourth point is that *there is offensive content on the Internet*. He is concerned about a wide availability of all kinds of pornography on the Internet, while he is aware that almost all of this is legal and a free society should permit access to such material, and claimed that "many Internet users want to place some limitation on access to such material." Another argument is that *there is criminal activity on the Internet.* Thus, "society is entitled to protect itself by enforcing the criminal law in relation to online activity."

However, I cannot agree with Darlington's arguments. His first argument is weak because the Internet is not open to everybody. There are already various barriers on the Internet. There have been significant disparities of the Internet access rate not only between nations, but also between social strata.[16] As discussed above, a large number of the global population, mainly from many developing nations, have been excluded from access to the Internet for socio-economic reasons.

Secondly, I take issue with Darlington's claim that the Internet is no different from other electronic networks. In a sense, the Internet has characteristics of broadcast media. However, it does not necessarily mean that it is a broadcast medium. In this context, it does not need to be regulated in the same way that broadcast media is regulated – this issue will be discussed in depth through a case study of *the Communications Decency Act* (CDA) 1996 in Chapter 2 (see Chapters 2.6.1.1). The Internet has integrated all kinds of existing communication technologies into itself. It is a medium which is still growing. Thus, issues over an affirmative definition of this new medium are still under discussion.

Thirdly, Darlington does not provide a clear definition of harmful content. He mentioned child pornography as an example of harmful Internet content. In my view, it would be classified as illegal content rather than harmful content. This is an important issue, because the ways to deal with harmful content and with illegal material are significantly different. While governments and legal authorities have directly dealt with illegal Internet content, multi-layered regulatory efforts have been applied to harmful but legitimate content (see Chapters 3.5).

---

[16] For more details, see *Falling through the Net: Defining the Digital Divide* (US Department of Commerce, 1999).

The above arguments show that the development of the Internet has highlighted controversial issues concerning freedom of expression and regulation. It has been argued that certain information on the Internet needs to be regulated but it has also been argued that the Internet is independent of governmental interventions.

The question about a feasible practice to deal with these issues still remains to be solved. In order to answer to this question, this thesis critically appraises trends in Internet content regulation and the method of dealing with illegal and harmful Internet material.

In Chapters 2 the theoretical issues relating to freedom of expression and regulation on the Internet are discussed. The chapter begins with a study of International declarations and conventions which have confirmed freedom of expression as an essential human right. This discussion appraises the importance of free speech rights, but also identifies that such rights are not absolute. They are restricted for a variety of reasons, such as issues of obscenity. Therefore, freedom of expression incorporates a certain degree of responsibility. In this context, the thesis argues that the Internet does not operate in a legal vacuum because it is subject to a legal framework. This thesis then discusses the definitions of illegal and harmful content. They are also considered with reference to South Korea. A few relevant South Korean judicial precedents are reviewed in this discussion.

After that, debates over freedom of expression and governmental Internet content regulation are critically appraised through six key case studies: *the Communications Decency Act* (CDA) and *the Child Online Protection Act* (COPA) in the US, *the Broadcasting Services Act* in Australia, a series of Internet Regulations in China from 1996 to 2000 and the co-regulatory model

in the UK and the EU. Through the case studies, the thesis identifies the limitations of geographically bound government regulations that cannot function properly in the global Internet environment, although they are effective in regulating illegal Internet content.

Chapter 3 discusses both theoretical and practical aspects of self and co-regulation. The chapter begins with a preliminary discussion about the general definition of self-regulation. Advantages and drawbacks of self-regulation are considered in terms of Internet content regulation. This chapter also discusses the EU's co-regulatory model, the 'Action Plan on Promoting of Safer Use of the Internet.' Furthermore, two of Internet content self-regulatory institutions in Europe, the Internet Watch Foundation, UK and INHOPE are critically appraised.

In Chapters 4 and 5, detailed technical reviews and critiques of the current Internet content filtering software and PICS-based Internet content rating systems are conducted. In particular, two US legal cases, *Mainstream Loudoun v. Board Trustees of the Loudoun County Library* (1998) and *ALA v. US* (2000), that deal with filtering software issues are discussed. Ten stand-alone filtering software products are reviewed in order to examine how the filtering technologies are applied to commercial products in practice. Three leading Internet content rating systems, SafeSurf, RSACi and ICRA, are examined.

From Chapter 6 to 9, close attention is paid to Internet content regulation in South Korea, my home country, which is referred to as the most wired nation in the world (Fulford, 2003). In Chapter 6 South Korea's significant Internet usage and infrastructure are explored and detailed statistics relating to Internet use are critically examined. A number of factors relating to the explosive development of the Internet, ranging from cultural aspects to governmental

policy, are discussed. A mandatory Internet content rating system in use in South Korea is analysed and situated within a broader context in Chapter 7. Chapter 8 researches its impacts on actual Internet content through two case studies, EXZONE.COM and iNOSCHOOL.NET, and through a special survey conducted by the author. As the conclusion of the case study of South Korea, Chapter 9 focuses on issues of the Internet content policy. This chapter analyses the South Korean Constitutional Court's decision[17] that held the major Internet content regulation unconstitutional. Issues relating to the implementation of the Internet content regulation policy proposal in South Korea are also discussed.

Finally, in Chapter 10, the thesis concludes by discussing the potential of better solutions to the issues of freedom of expression and regulation on the Internet. The drawbacks of the existing co-regulatory model are discussed, including risk of self-regulation, limitation of International consent and defects of technical solutions. The conclusion of this thesis develops ways forward for the future of Internet content regulation. A collective regulatory model is presented which takes into account the experiences of Internet content regulation in Europe and South Korea.

[17] Judgment of June 27, 2002, 99Hun-Ma480, 14-1 KCC 616. see Chapter 9.2.

CHAPTER 2

FREEDOM OF EXPRESSION AND REGULATION ON THE INTERNET

2.1. Declarations and Conventions on Freedom of Expression

John Stuart Mill wrote in his essay, *On Liberty*, that:

> The time, it is to be hoped, is gone by when any defence would be necessary of the 'liberty of the press' [...] (Mill, 1859/1974, p. 75)

Freedom of expression is one of the basic human rights, and a fundamental part of the modern democratic process.[1] In the 17th century John Milton argued that freedom of expression is the most valuable of all the freedoms which human beings may have. He fought against the pre-publication licensing law of his day. He stated in his article *Areopagitica*:

> Give me the liberty to know to utter, and to argue freely according to conscience, above all liberties (Milton, 1644/1951, p. 49).

His thinking underpins the fundamental philosophy of the First Amendment to the American Constitution and has influenced the constitutions of many modern democratic countries. Historically, the First Amendment to the US Constitution,[2] which was ratified in December 1791, was an important

---

[1] Barendt (1985) discussed that a free speech principle has been based on three major arguments over the importance of open discussion to the discovery of truth, each individual's right to self-development and fulfillment, and citizen participation in a democracy. Firstly, "if restrictions on speech are tolerated, society may prevent the ascertainment and publication of true facts and accurate judgments." (p. 8) Secondly, "people will not be able to develop intellectually and spiritually, unless they are free to formulate their beliefs and political attitudes through public discussion and in response to the criticism of others." (p. 14) Thirdly, he stated that the argument from citizen participation in democracy is "the most attractive and certainly most fashionable free speech theory in modern Western democracies" (p. 20) in terms of protecting the right of all citizens to understand political issues so as being able to participate effectively in the working of democracy.

[2] The first written constitution, the US Constitution, was signed in September 1787. However, arguments between the Federalists and the Anti-federalists, and the fear that the Constitution might jeopardise individual rights meant that some states did not ratify the Constitution. Consequently, the first US Congress proposed to the state legislatures amendments to the

milestone in terms of giving legal recognition to the importance of the idea of freedom of expression:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances (Amendment I).

Over the past century, freedom of expression as an essential human right has been confirmed through numerous international and regional declarations and conventions, including the Universal Declaration on Human Rights, the European Convention on Human Rights, and the International Covenant on Civil and Political Rights.

After the Second World War, during which people experienced fascist regimes' violations of the most basic human rights, the international community proclaimed an urgent need for international protection for some basic standard of human dignity and worth. From April 1946 the United Nations Commission

---

Constitution in 1789. The US Information Agency describes the history of the Bill of Rights in its publication, *An Outline of American History* (Cincotta, 1994), as follows:

> By June 1788 the required nine states ratified the Constitution, but the large states of Virginia and New York had not. [...] Differing views on these questions brought into existence two parties, the Federalists, who favored a strong central government, and the Antifederalists, who preferred a loose association of separate states. [Another] concern to many was the fear that the Constitution did not protect individual rights and freedoms sufficiently. Virginian George Mason, author of Virginia's 1776 Declaration of Rights, was one of three delegates to the Constitutional Convention who refused to sign the final document because it did not enumerate individual rights. [Therefore, when] the first Congress convened in New York City in September 1789, the calls for amendments protecting individual rights were virtually unanimous. Congress quickly adopted 12 such amendments; by December 1791, enough states had ratified 10 amendments to make them part of the Constitution. Collectively, they are known as the Bill of Rights.

on Human Rights[3] began to work on a document named the Universal Declaration of Human Rights.[4] In 1948 the General Assembly of the United Nations adopted it without dissent (Johnson, 1998). It declares that "all human beings are born free and equal in dignity and rights" (Article 1) and its Article 19 proclaims:

> Everyone has the rights to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Although the Universal Declaration monumentally confirmed the international norm of freedom of speech, it has no compelling power itself, since it is not a treaty. Nevertheless the Universal Declaration has inspired other declarations and agreements on human rights for the past half-century.

In 1950, as a response to the Universal Declaration on Human Rights, the Council of Europe drew up the European Convention on Human Rights.[5] It is one of the most important regional conventions which European nations have adopted in order to secure basic human rights. It consists of 66 articles including a preamble and 11 protocols, and imposes much more powerful

---

[3] The four main players of the Commission who participated in producing the Declaration were as follows: Eleanor Roosevelt of the US, the Chair of the Commission; P. C. Chang of China, the Vice-Chair of the Commission; Charles Malik of Lebanon, the Rapporteur; and René Cassin of France.

[4] The full text of the Declaration is available on the Office of the UN High Commissioner for Human Rights Website at http://www.unchr.ch/udhr/lang/eng.htm (Retrieved February 17, 2005)

[5] The full text of the European Convention on Human Rights is available on the Council of Europe Website at http://www.echr.coe.int/Convention/webConvenENG.pdf (Retrieved February 21, 2005)

structures as compared to the Universal Declaration (Weil, 1963, pp. 21-40).[6] Article 10 (1) of the European Convention, which reiterates Article 19 of the Universal Declaration, also declares the right of free speech:

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers [...]

With regard to Article 10 of the European Convention, the European Court of Human Rights claimed, "Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man."[7]

By the General Assembly of the United Nations, the International Covenant on Civil and Political Rights[8] was announced in 1966. According to a report from the Office of the UN High Commissioner for Human Rights (2004), the Covenant has been ratified by 152 nations world wide as of June 2004. On 10th July 1990, South Korea acceded to the Covenant. The International Covenant restates the right of free speech in its Article 19 as follows:

---

[6] Article F(2) of the Treaty on European Union reads:

> The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms [...] and as they result from the constitutional traditions common to the Member State, as general principles of Community law.

[7] The case of *Handyside v. the United Kingdom* (1976) Series A No. 24. In the *Handyside* judgment of 7th December 1976, the Court found that prosecution under Obscene Publication Acts 1959 and 1964 for possession of the Little Red Schoolbook was a legitimate protection of morals.

[8] The full text of the International Covenant on Civil and Political Rights is available on the Office of the UN High Commissioner for Human Rights Website at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (Retrieved February 21, 2005)

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

2.2. Responsibilities of Freedom of Expression

However, in the real world, even in democratic societies, freedom of expression is not an absolute right. It has been restricted for a variety of reasons ranging from issues of national security to obscenity. Laws relating to defamation, incitement to racial hatred, contempt of court, protection of confidences and copyright have also limited it. For instance, in the UK a number of provisions restrict the freedom to express views and ideas which involve racial hatred, such as the Race Relations Act 2000.[9] Even the Universal Declaration clearly issues exceptions on freedom of expression in its Article 29(2):

> In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality,

---

[9] According to the Commission for Racial Equality (CRE) which is a publicly funded, non-governmental body set up under the Race Relations Act 1976:

> The Race Relations Act 1976, as amended by the Race Relations (Amendment) Act 2000, makes it unlawful to discriminate against anyone on grounds of race, colour, nationality (including citizenship), or ethnic or national origin. The amended Act also imposes general duties on many public authorities to promote racial equality. [...] Racist incidents ranging from harassment and abuse to physical violence are offences under the criminal law. Inciting racial hatred is also a criminal offence. Publishing and disseminating materials such as leaflets and newspapers that are likely to incite racial hatred is also a criminal offence (Commission for Racial Equality, 2001).

The Full text of the Race Relations (Amendment) Regulation 2003 is available at the Home Office's Website, http://www.homeoffice.gov.uk/docs/racerel1.html (Retrieved June 2, 2004)

public order and the general welfare in a democratic society.

The European Convention on Human Rights emphasises the responsibilities of the right to free speech in its Article 10 (2) as follows:

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Although this Article makes the condition that any restriction on the exercise of freedom of expression must be "prescribed by law" and "necessary in a democratic society," it admits certain restrictions which have "legitimate aims."[10] They fall into the following three categories: those designed to protect the public interest; those designed to protect other individual rights; [and] those that are necessary for maintaining the authority and impartiality of the judiciary (Directorate General of Human Rights, 2000). If these conditions are not fulfilled, a limitation on freedom of expression will amount to a violation of the Convention.[11] The Global Internet Liberty Campaign (GILC, 1998) argues that

---

[10] The European Court of Human Rights has applied this three-part test. It stated, "The Court therefore has to examine whether the interference [...] was 'prescribed by law,' whether it had an aim or aims that is or are legitimate under Article 10 (2) [...] and whether it was 'necessary in a democratic society' for the [...] aim or aims." (The case of *the Sunday Times v. the United Kingdom* (1979) Series A No. 30 §45)

[11] In the case of *Castells v. Spain* (1992, Series A No. 236), the European Court of Human Rights found that Article 10 had been violated, since "an interference in the exercise of the applicant's freedom of expression was not necessary in a democratic society." (§48) The applicant, Miguel Castells, an opposition Member of Parliament, published an article which criticised the inactivity of the government with regard to numerous attacks and murders that had taken place in the Basque Country. Criminal proceedings were instituted against the

Article 10 should be interpreted in light of other Articles, including Article 6—Right to a fair trial, Article 8—Right to respect for private and family life, and notably Article 17—Prohibition of abuse of rights.

In this context, the European Court of Human Rights has made a number of considerable judgments as regards Article 10,[12] such as *Handyside*,[13] *Müller and others*[14] and *Otto-Preminger-Institut*[15] judgment. In these cases, the Court held that the State might validly interfere with freedom of expression under the conditions laid down in Article 10(2), in particular the protection of morals and the protection of the rights of others. However, the Court stated that the exceptions in Article 10(2) "must be narrowly interpreted and the necessity for

---

applicant for insulting the Government, his parliamentary immunity was withdrawn, and he was convicted and sentenced to conditional imprisonment.

[12] A full text of the case law of the European Court of Human Rights is available through its Web database at http://www.echr.coe.int/Eng/Judgments.htm (Retrieved February 22, 2005).

[13] see Chapter 2: Footnote 7.

[14] The case of *Müller and others v. Switzerland* (1988) Series A No. 133. This case is about conviction and sentence to a fine for publishing obscene material following an exhibition of paintings, and confiscation of the mentioned paintings. In the *Müller and others* judgment of 24th May 1988, the Court stated, "[T]he paintings in question depict in a crude manner sexual relations, particularly between men and animals [...] the painting were displayed in an exhibition which was unrestrictedly open to [...] the public at large."(§36) and concluded, "In the circumstances, having regard to the margin of appreciation left to them under Article 10 §2, the Swiss courts were entitled to consider it 'necessary' for the protection of morals to impose a fine on the applications for publishing obscene material." (§36) The Court also held that the confiscation of the paintings did not infringe Article 10.

[15] The case of *Otto-Preminger-Institut v. Austria* (1994) Series A No. 295-A. The Otto-Preminger-Institut, which runs a licensed cinema, intended to screen the film Das Liebeskonzil (Council in Heaven) which is based on Oskar Panizza's controversial (and allegedly strongly anti-Catholic) theatre play. The Innsbruck Regional Court acting on a complaint submitted by the Roman Catholic diocese of Innsbruck prohibited the Otto-Preminger-Institut from showing the film and ordered the seizure of the film on suspicion of the attempted criminal offence of disparaging religious precepts (Section 188 of the Austrian Penal Code). In the *Otto-Preminger-Institut* judgment of 20th September 1994, the Court stated, "The Government maintained that the seizure and forfeiture of the film were aimed at 'the protection of the rights of others,' particularly the right to respect for one's religious feelings, and at 'the prevention of

any restrictions must be convincingly established."[16] Indeed, in practice, freedom of expression has come into conflict with other human rights and interests such as the individual's right to privacy.[17] For this reason governments have been allowed to regulate speech which may violate human rights. The European Commission (1996a) stated that:

> Freedom of expression may be restricted by the State, though the possible restrictions are circumscribed by a very precise set of criteria: to be considered necessary in a democratic society, the measure must meet a real social need and be effective without being disproportionate in the restrictions it imposes. The assessment will require the proportionality test to be applied.

Nowadays, in modern democratic countries the judiciary decides whether speech is lawful or not. However, issues about the freedom of speech often remain controversial. Barendt (1985, pp.2-3) argues that:

> The function of courts in [free speech] cases raises notoriously difficult questions. [It is] almost impossible to draw a clear line between legal and philosophical or political argument for the disposition of such litigation. [...] The courts' tasks when construing [free speech] provisions [such as Article 5 of the German Basic Law[18] or Article 10

---

disorder'" (§46) and held that there has been no violation of Article 10 of the Convention as regards either the seizure or the forfeiture of the film.

[16] The case of *the Sunday Times v. the United Kingdom (no. 2)* (1991) Series A No. 217. §50(a)

[17] The European Convention on Human Rights issues the right to respect for private and family life in its Article 8 (1), "Everyone has the right to respect for his private and family life, his home and his correspondence."

[18] Article 5 of the Basic Law for the Federal Republic of Germany [Freedom of expression]

> (1) Every person shall have the right freely to express and disseminate his opinions in speech, writing, and pictures and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.

of the European Convention on Human Rights] remains fundamentally different from that imposed in the process of ordinary statutory interpretation.

2.3. The Internet is not a Legal Vacuum

On the Internet these issues become ever more debatable, because of the unique attributes of the Internet, such as decentrality and transnationality, as discussed in Chapter 1. The characteristics of the Internet have made it an interactive global medium. Issues over freedom of expression and regulation on the Internet are highly contentious and hard to compromise. In the battle over free speech rights and regulation on the Internet, there are two significant viewpoints. On the one hand, some Internet libertarians, such as John Perry Barlow, claim unlimited freedom of expression and object to any legal restrictions on the Internet and argue that any Internet regulation will inevitably lead to some degree of governmental intervention. On the other hand, people and institutions, such as the Internet Watch Foundation (IWF), insist, "The Internet is not a legal vacuum." (ISPA UK, LINX & the Safe-Net Foundation, 1996) They doubt the efficacy of the marketplace of ideas on the Internet, and argue that there is an urgent need for a new regulatory framework. In the following section I will discuss these two viewpoints.

John Barlow (1996b) argues in his article, *A Declaration of the Independence of Cyberspace* that the Internet is naturally independent as follows:

> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself

(2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour.
(3) Art and scholarship, research, and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution.

> always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Barlow argued that the Internet is uniquely resistant to governmental controls and has a great capacity to promote democracy worldwide, since its fundamental characteristics have made it a unique communication medium. Some Internet enthusiasts, such as Howard Rheingold, have considered the advent of the Internet as a revitalisation of the ideal public sphere which is transparent and accessible for all citizens, thus public opinions can be openly and freely discussed and formed. Rheingold has played a main role in developing utopian visions of the Internet and claims that it could help citizens revitalise democracy:

> We temporarily have access to a tool that could bring conviviality and understanding into our lives and might help revitalise the public sphere [...] the vision of citizen-designed, citizen-controlled worldwide communications network is a version of technological utopianism that could be called the vision of "electronic agora." (Rheingold, 2000, pp. xxx)

Mitchell also upholds the idea of "electronic agora" in his book, *City of Bit* (1995, p. 8), as follows:

> [The Internet] will play as crucial a role in twenty-first-century urbanity as the centrally located, spatially bounded, architecturally celebrated agora did (according to Aristotle's Politics) in the life of the Greek polis [...]

However, this idealism concerning the Internet has been strongly criticised. Haywood argues that the marketplace of ideas is not working on the Internet:

> Access to these networks will simply be laid over the same old pattern of geographic and economic inequality. [...] the network as a marketplace of ideas will move from metaphor to reality where established patterns of consumer detriment, the compounded disadvantages of low-income group, are replicated in digital form. [...] Social divisions and distinctions have remained largely untouched by the massification of a whole range of computer-based technologies, and the Internet will be no different (Haywood, 1998, pp. 22-23).

In reality, the incredible success of the Internet has been proportionate to the development of its more negative aspects such as cyber fraud and distribution of obscene materials. This shows that a variety of dangers exist on the Internet just like in the real world. Sometimes, because of its characteristics, such as anonymity, the problems on the Internet are more complicated than the equivalent problems in the 'real' world. It is also harder to find effective solutions for them. Since the unique characteristics of the Internet have enabled end-users to directly control content and significantly reduced media costs, the information and communications environment has been drastically changed. As a result, new kinds of social and legal problems have occurred. In my view, it can be argued that a new regulatory approach is necessary which takes into account the unique characteristics of the Internet.[19] Hence, some degree of carefully circumscribed regulation on the Internet is inevitable as our society is being subject to a certain legal framework, in particular as regards obscenity, defamation of character and other such aspects that are not protected by law. The Internet cannot be a lawless place just as IWF argued earlier. In reality most governments all over the world regulate the Internet in a variety of ways.

[19] For instance, in order to address issues of Internet pornography, UK obscenity legislation has been amended by the Criminal Justice and Public Order Act 1994 (Akdeniz, 1997a, p. 226. see Chapter 2.6.4.1).

2.4. Regulating Illegal and Harmful Content on the Internet

Nevertheless, regulating the Internet is not an easy task. Issues of jurisdiction and territorial rights are such examples, since "the cost and speed of information transmission on the Internet is almost entirely independent of physical location." (Johnson & Post, 1996) Increasing globalisation presents similar challenges. Since each country or community has different criteria regarding what is inappropriate to the public, it is impossible to apply a common standard to the Internet. Indeed, much information on the Internet comes from outside jurisdiction[20] and consequently reflects very different — and often incompatible — moral, religious and political standards.

2.4.1. Illegal Content and Harmful Content

Content-related problems have been largely identified and categorised as illegal and harmful content (Akdeniz, 2001c, p. 303). As regards adult information, many countries, including the US and South Korea apply different criteria of indecent and obscene information to adults and minors. The concept of indecency is applied to minors, while the concept of obscenity is applied to

[20] In 2002 about 73% of Internet hosts were based in the US and this domination is likely to continue for some time.

	1998	1999	2000	2001	2002
US	30,489,463 (70%)	53,175,956 (74%)	80,566,947 (75.5%)	106,193,339 (75%)	115,311,958 (73%)
UK	1,449,315	1,739,078	1,677,946	2,230,976	2,865,930
World Total	43,545,197	72,005,852	106,710,508	141,615,267	157,581,802

The number of Internet hosts (Resource: The International Telecommunication Union: Statistics Web page. Retrieved July 7, 2004, from http://www.itu.int/ITU-D/ict/statistics/)

According to *Internet Infrastructure Indicators* by the Organisation for Economic Co-operation and Development (OECD), 94 of the100 most popular Websites on the Internet are based in the US (OECD, 1998). The Internet Watch Foundation reports that over 95 percent of the criminal content of the Internet originates outside the UK (IWF, 2001).

adults. In many countries indecency falls within the protection area of the right to free speech even if it is pornography, but obscenity is not legally protected. For instance, children's access to pornographic content and child pornography are significantly different issues. While the former may be harmful for their development, but may not be illegal for adults, the latter is subject to criminal punishment in most nations. In other words, indecent or potentially harmful content is subject to freedom of expression, even though some people may consider it as offensive, while illegal content is considered to be criminal. The European Court of Human Rights has confirmed this notion through its case law. In the *Handyside* judgment the Court stated:

> Freedom of expression [...] is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society." (The Case of *Handyside v. the UK* (1976) §49. see Chapter 2: Footnote 7)

In terms of Internet content regulation, the European Commission (1996b) stated that harmful content and illegal content are significantly different issues in nature which call for very different legal and technological responses. It claimed, "It would be dangerous to amalgamate separated issues." Therefore, they should be treated with different approaches respectively.

2.4.2. Illegal content

Illegal content can be defined as a certain type of content which is considered to be criminal, although its exact definition varies according to national laws which are based on cultural differences. This is the case, for example, with trafficking in human beings, dissemination of racist material or incitement to

racial hatred, terrorism or all forms of fraud. Among many kinds of illegal content, child pornography presents an example of clear-cut illegality in most countries worldwide. It is an area where a high degree of consensus exists within member nations of the European Union, even though the laws regarding child pornography also differ according to each nation (Akdeniz, 2000).

As Akdeniz (2001c, p.303) comments, the issue of illegal Internet content and how to deal with it has revolved around child pornography. The reason why child pornography is considered to be a serious criminal matter is that it is a form of sexual exploitation of children. A report of the US Department of Justice, known as *the Meese Report*, described child pornography as material which includes the sexual abuse of a real child. It claimed, "there can be no understanding of the special problem of child pornography until there is understanding of the special way in which child pornography is child abuse." (Attorney General's Commission on Pornography, 1986, p. 405) A proposal of the European Commission (2001b) states, "Sexual exploitation and child pornography constitute serious violations of human rights and of the fundamental right of a child to a harmonious upbringing and development."

In this context, the circulation of child pornography through the Internet has been of great concern to authorities and parents. Since the Internet provides anonymous global communications, its misuse by paedophiles was discovered even before the proliferation of the Internet in the early 1990s. According to *the Meese Report* in 1986, paedophile offenders and child pornographers had already begun to use personal computers for communications (Attorney General's Commission on Pornography, 1986, p. 629).

Another example of illegal Internet content is speech which involves racism or xenophobia. In many European nations, including Belgium, France and

Germany, racism and xenophobia are not subject to the right to free speech, but they are prohibited and penalised. Since the mid-1990s a number of people in these countries have been prosecuted for posting messages of a racist and xenophobic nature on the Internet (Frydman & Rorive, 2002). In November 2001, the European Council issued a 'proposal for Council Framework Decision on combating racism and xenophobia' which aimed at ensuring that racism and xenophobia are punishable in all EU Member States by criminal penalties (European Commission, 2002). However, in the US these kinds of speech are protected under the First Amendment as varieties of controversial political speech. According to the Simon Wiesenthal Centre,[21] in the year 2000 more than 2,300 Websites which contained racist or xenophobic messages were found to be hosted in the US. Among them more than 500 extremist sites were allegedly authored by Europeans (Perine, 2000). This is a prime example of one of the global features of the Internet; it creates "the possibility of particular countries becoming 'safe havens' for material which is in breach of the criminal laws of other countries." (ABA, 1997)

2.4.3. Harmful Content

There are significant difficulties in defining "harm", particularly at an international level. A document of the European Commission (1996b) defines harmful content as "various types of material" which may "offend the values and feelings of other persons." Akdeniz (2001c) argues that it is a form of content which may include "sexually explicit content, political opinions, religious beliefs, views on racial matters and sexuality," but also points out that

[21] The Simon Wiesenthal Center is an international Jewish human rights organisation which is accredited as an NGO both at the UN and UNESCO. It was established in 1977 and its head office is in Los Angeles. More information about the centre is available on its Website, http://www.wiesenthal.com (Retrieved March 18, 2005).

the criterion of harmful content differs even within member States of the European Union. For instance, in the case of *Handyside v. the UK*, Mr. Richard Handyside was prosecuted under Obscene Publication Acts 1959/64 (UK) for possession of the Little Red Schoolbook which circulated freely in other European countries (see Chapter 2: Footnote 7). Therefore, the European Commission (1996b) states:

> What is considered to be harmful depends on cultural differences. Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible.

In this context, the European Court of Human Rights has held that governments are allowed a "margin of appreciation" to determine whether a restriction on freedom of expression is necessary in light of local circumstances through its case-law (see Chapter 2: Footnote 7, 14, 15).

Consequently, certain information which is deemed to be harmful in one country is not necessarily considered to be harmful in other countries. Following the same argument, a certain type of illegal information in one country can be legitimate in other countries. The Internet environment, which has provided people with the free flow of information worldwide, has made these issues more complicated than the equivalent problems in the real world. On the one hand, there are legal frameworks working at an international level which seek to harmonise national laws against illegal content, in particular child pornography, for example, 'Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.'[22] On the other hand, there are certain grey areas between illegal

[22] On 26th May 2000, the UN General Assembly adopted the 'Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.' It ensures special attention to the criminalisation of these serious violations of

and harmful content, as mentioned in the case of racism and xenophobia (see Chapter 2.4.2).

Although, as discussed above, it is unfeasible to make an affirmative definition of harmful Internet content at an international level, for this study I shall understand harmful Internet content as various types of Internet content which may violate others' moral, religious or political opinions and belief, therefore which may be subject either to freedom of expression and to governmental sanctions depending on a given jurisdiction's appreciation. Making a clear distinction between illegal and harmful content is crucial to this thesis which aims to explore the issues relating to content regulation and freedom of expression on the Internet. In the following section, the issues of illegal and harmful content, in particular obscene and indecent content, will be discussed further with special reference to South Korea. This will also be a preliminary discussion for the study of the Internet content regulation in South Korea.

2.5. Freedom of Expression in South Korea

Before discussing any issue which is related to freedom of expression in South Korea, it is necessary to consider South Korea's political background. In South Korea, during the period of military dictatorship and authoritarian rule of Bak Jeong-Hui (1961-1979) and Jeon Du-Hwan (1980-1987), suppression of freedom of expression was very severe, since "freedom of expression was

---

children's rights and emphasizes the importance of fostering increased public awareness and international co-operation in efforts to combat them (UNICEF, 2000). South Korea signed the Optional Protocol in September 2000 (Office of the UN High Commissioner for Human Rights, 2004).

The full text of the Optional Protocol is available on the Office of the UN High Commissioner for Human Rights Website at http://www.unhchr.ch/html/menu2/dopchild.htm (Retrieved March 15, 2005).

tantamount to permitting criticism of those in power." (Chong, 1999, p.241) On 17th October 1972, Bak Jeong-Hui who took over the government by a coup d' état in May 1961, proclaimed martial law, dissolved the National Assembly and suspended all political activities. Ten days later, a draft of the YUSIN (literally, 'revitalization') Constitution was put to a national referendum which allowed Bak to remain in control indefinitely.[23] Bak was assassinated by Kim Jae-Gyu, the head of JUNGANG JUNGBOBU (Korean Central Intelligence Agency), in October 1979. Just two months later, General Jeon Du-Hwan took power by another coup d' état, and his regime killed hundreds of civilians in KWANGJU who protested against the coup in May 1980 (Office of the UN High Commissioner for Human Rights, 2003; Savada & Shaw, 1992). Throughout the 1980s the pro-democracy movement intensified, culminating in 1987, a landmark year in the history of Korean democracy. After a massive citizens' protest of June 1987, known as YUWOL HANGJANG (June Struggle), Jeon's regime agreed to democratic reforms, including a constitutional amendment for restoring direct presidential election. However, in 1987, under the new Constitution, Roh Tae-Woo, a former four-star general who played a major role in the 1980 coup, was elected President by a slim margin, mainly because his opposition was split between two civilian leaders, Kim Yeong-Sam and Kim Dae-Jung. In 1992, Kim Yeong-Sam was elected President and formally opened the civilian form of government.[24] Kim Dae-Jung, who was awarded a Nobel Peace prize in 2000, won the presidential election held in December

[23] Under the Yusin Constitution, Bak Jeong-Hui was re-elected as the president by the Tongil Juche Gungmin Hoeui (National Conference for Unification) and one-third of the National Assembly members was appointed by Bak. In November 1972 the Yusin Constitution was confirmed by the referendum (Savada & Shaw, 1992).

[24] In 1995 Jeon and Roh were found guilty of treason, murder, bribery and other crimes and sentenced to death and life imprisonment respectively (Judgement of April 17, 1997, 96 Do3376, Daebeopwon [Supreme Court]). However, they were pardoned by President Kim Yeong-Sam in 1997 (C. Kim, 2000).

1997. This was the first democratic turnover from a ruling to an opposition party in South Korea (C. Kim, 2000; Office of the UN High Commissioner for Human Rights, 2003; Yang, 2000). In this context, Professor Ahn Kyong-Whan (1997, p.115) states,

> Korea is undergoing a rapid transformation in many ways: from an authoritarian society to a democratic one, from a non-litigious society to a litigious one, and from a country with a decorative constitution to a country with a working constitution.

The current South Korean Constitution[25] guarantees freedom of expression and the press in its Article 21(1) and 21(2).

> (1) All citizens shall enjoy freedom of speech and the press, and freedom of assembly and association; (2) Licensing or censorship of speech and the press, and licensing of assembly and association shall not be recognized.

Furthermore, Article 22(1) confirms all citizens' freedom of learning and the arts. Article 37(1) protects people's basic freedom and rights from being disregarded on the grounds that they are not enumerated in the Constitution. Youm Kyu-Ho (2001, p. 42) argues that the explicit prohibition of prior censorship on freedom of expression under Article 21(2) is a significant improvement on the Constitution of 1980 which did not forbid censorship of expression. However, the Constitution also contains broad and clear restrictions on exercising freedom of expression. Article 21(4) reads, "Neither speech nor the press shall violate the honour or rights of other persons nor undermine

[25] On July 17, 1948, the first Constitution of the Republic of Korea was adopted. Since then, the Korean Constitution has been amended nine times, with the October 29, 1987 amendment being the latest. The full text of the Constitution is available in English on the Constitutional Court of Korea Website at http://www.ccourt.go.kr/english/welcome01.htm (Retrieved February 26, 2005).

public morals or social ethics." Article 37(2) also states, "The freedoms and rights of citizens may be restricted by Act only when necessary for national security, the maintenance of law and order or for public welfare."

In terms of the obscenity and indecency debate, the phrase "undermine public morality or social order" in Article 21(4) has been a common justification for regulations on sexual expression in South Korea. Moon Jae-Wan at Dankook University in Seoul claims, "Legislative invocation of a concern for public morals is usually a politically popular justification for government regulation." (Moon, 2003, p. 356) South Korea has a number of statutes which regulate obscene materials with panel provisions, including *HYEONGBEOP* [*Criminal Act*], *JEONGI TONGSIN GIBONBEOP* [*Framework Act on Telecommunications*] and *JEONGI TONGSIN SAEOPBEOP* [*Telecommunications Business Act*].[26]

Article 243 and 244 of *the Criminal Act*[27] have been a legal foundation for regulating obscenity of the traditional print media in South Korea, while Article 48(2) of *the Framework Act on Telecommunications* and Article 53 of *the Telecommunications Business Act* have regulated obscene materials on the Internet. However, there have been arguments which claim these statutes' definitions of obscenity is vague. Indeed, although obscenity has long been

---

[26] *The Framework Act on Telecommunications* and *the Telecommunications Business Act* will be discussed further in Chapter 7.

[27] Article 243 and 244 of the Criminal Act reads as follows:

> [Article 243] A person who disseminates, sells, leases, or makes public displays of obscene writings, visual images, films, and other materials shall be punished by imprisonment for not more than one year or by a fine not exceeding 5 million KRW.
> [Article 244] A person who makes, possesses, imports, or exports obscene materials in order to practice activities of Article 244, shall be punished by imprisonment for not more than one year or by a fine not exceeding 5 million KRW.

The full text of the Criminal Act is available in Korean on Beopjecheo (the Ministry of Government Legislation Website at http://www.moleg.go.kr/ (Retrieved March 1, 2005).

used as a legal term by a number of statutes, no statute has defined obscenity yet (Jong S. Kim, 2003 p.216; Moon, 2003, p. 358). In 1996 a lawsuit which questioned the constitutionality of Articles 243 and 244 of *the Criminal Act* was filed in the Korean Constitutional Court. The petitioner claimed that these Articles were unconstitutional because the definition of obscenity in *the Criminal Act* was ambiguous, but the Court dismissed the petitioner's claim,[28] because he did not adhere to a deadline regarding the timing of the legal proceedings of *the Constitutional Court Act.*[29] Furthermore, the Constitutional Court held Article 53 of *the Telecommunications Business Act* to be unconstitutional, because the way in which concept of "improper communication" is defined is too vague.[30] This judgment was significant for Internet content regulation in South Korea, because the Court set the precedent for restraining the government-centred Internet content policy. This will be discussed in depth in Chapter 9.2.

While in terms of the rule of clarity these statues' definition of obscenity has been muddled, a number of precedents have established jurisprudence of obscenity. In 1995 the Supreme Court articulated the most comprehensive

---

[28] Judgment of November 27, 1997, 96Hun-Ma103.

[29] Article 69(1) of *the Constitutional Court Act* reads as follows:

> A constitutional complaint under Article 68 (1) shall be filed within sixty days after the existence of the cause is known, and within one hundred eighty days after the cause occurs: Provided, That a constitutional complaint to be filed after taking prior relief processes provided by other laws, shall be filed within thirty days after the final decision in the processes is notified.

The full text of *the Constitutional Court Act* is available in English on the Constitutional Court Website at http://www.ccourt.go.kr/english/welcome02.htm (Retrieved March 3, 2005).

[30] The Korean Constitution Court's decision on the Ban on Improper Communication on the Internet case (14-1 KCCR 616, 99HUN-MA480, June 27, 2002).

obscenity test in the *JEULGEOUN SARA* [*Happy Sara*] case:[31]

> Whether a document is obscene should be determined by considering the explicit and graphic depiction of sex, the amount and substantiality of the sexual description in relation to the document as a whole, the ideas expressed in the document and their relationship to the sexual portrayal, the lessening impact of the document's artistic and theoretical values on its sexual titillation. Further, examination should be made of whether the document, taken as a whole, primarily appeals to readers' prurient interest. After all of these factors are considered altogether, the document, applying the wholesome contemporary social custom, should be evaluated to find whether it stimulates sexual desires for no special reason and whether it affronts an average person's proper sense of shame about sex and violates the sound morality on sex.

However, Cho Kuk (2003, pp. 142-146), a professor at Seoul National University, argues that the Supreme Court's definition of obscenity is based on morality rather than any other standards, such as artistic merit or ideology. According to the Supreme Court's obscenity test, Cho Kuk argues that criminal sanctions are tie to the moral standards of society, if "a material as a whole is judged to appeal to the prurient interest by containing detailed and offensive sexual depiction and description." (p. 161) As we see in the *Happy Sara* case[32] and the *NAEGE GEOJINMALEUL HAEBWA* [*Lie to Me*] case,[33] a number of

---

[31] *Ma Kwang-Su v. State*, 94DO2413, Judgment of June 16, 1995, DAEBEOPWON [Supreme Court]. The novel *Happy Sara* was published in 1992, written by a well-known literature professor Ma Kwang-Su at YONSEI University in Seoul. The novel raised controversy because of its frank description of sexual bevaviour. Professor Ma was prosecuted for violating Article 243 and 244 of *the Criminal Act*. On 18th December 1992 the trial court held that the novel *Happy Sara* was obscene and sentenced him to eight months imprisonment with probation for two years. The appellate court affirmed the conviction (Judgment of July 13, 1994, 93NO446, Seoul HYEONGSA JIBANG BEOPWON [Seoul District Criminal Court]). The Supreme Court finally dismissed the appeal.

[32] *Ibid.*

[33] *Jang Jeong-Il v. State*, 98DO679, Judgment of October 27, 2000, DAEBEOPWON [Supreme Court]. On 13th January, 1997, Jang Jeong-Il, a popular writer, was prosecuted for violating

literature and artistic expressions have been punished as obscene, because the Supreme Court has considered artistic value or concept of a literary work only as one of many points to be considered in its obscenity test.

In the same year the Korean Constitutional Court articulated a more distinctive definition of obscenity and indecency in the case on *Registration Revocation of Obscenity Publishers.*[34] The Constitutional Court respected the Supreme Court's viewpoint, but gave a different definition of obscenity. The Court stated that:

> Obscenity is a sexually blatant and undisguised expression that distorts human dignity or humanity. It only appeals to prurient interests and, if taken as a whole, does not possess any literary, artistic, scientific, or political value. Obscenity not only undermines the healthy societal morality on sex, but its harmful impact is also difficult to eliminate through the mechanism of competition of ideas. Accordingly, obscene expression, if strictly interpreted as suggested here, is not within the area of constitutionally protected speech or press.

When compared with the Supreme Court's definition, Professor Cho (2003) argues that the Constitutional Court provided a "liberal" standard of obscenity. Unlike the Supreme Court, it defines obscenity as sexual expressions which destroy "human dignity or humanity" and emphasises on the role of "the mechanism of competition of ideas" before punishing obscene materials.

Article 243 and 244 of *the Criminal Act* for his novel, *Lie to me*, which frankly describes various types of sexual behaviours, including masochism and sadism. The trial court sentenced him to one year imprisonment. Just like the *Happy Sara* case, the appellate court affirmed the trial court's decision (Judgment of February 18, 1998, 97No4055, Seoul JIBANG BEOPWON [Seoul District Court]) and the Supreme Court finally dismissed Jang's appeal.

[34] Judgment of April 30, 1998, 10-1 KCCR 327, 95HUN-KA16. This case reviewed constitutionality of a statute which authorises revocation of a publisher's registration for publishing obscene or indecent materials. The court upheld revocation of registration for obscenities, but ruled that the same for indecencies is unconstitutional.

Alongside its definition of obscenity, the Constitutional Court clarifies indecency as "a sexual or violent and cruel expression, a swearing, or other expression of vulgar and coarse content," which does not reach "the level of obscenity" and remaining with "the domain protected by the Constitution." However, the Court concedes, "The concept of indecency is so broad and abstract that a judge's supplementary interpretation cannot sharpen its meaning."[35] The Constitutional Court's judgment was significant in that it defined permissible sexual expression for the first time. Youm (2002, p. 143) applauds the Court's effort to distinguish obscenity from indecency. He wrote, "The Constitutional Court applied its free speech principles in determining whether the government can restrict obscenity without violating the Constitution."

The Court states, "There is a definite need to regulate decadent sexual expressions or excessively violent and brutal expression to protect juveniles' healthy minds and sentiments." However, the Court held, "such regulation should be limited to juveniles and narrowly tailored to prohibit the dissemination of the indecent material." Otherwise, the Court warned that adults' "right to know" would be violated, because a total banning on indecent materials is "excessive as a means for juvenile protection" and "forces adults' right to know to conform to adolescent standards."[36] As we discussed above, the Korean Constitutional Court clearly differentiates obscenity from indecency and takes separate approaches to tackle each issue. First of all, the Court affirms that, as regards regulation of indecent and harmful content, the primary regulatory mechanism is inherent in civil society in the name of

---

[35] *Ibid.*

[36] *Ibid.*

competition of ideas, and therefore governmental intervention should be minimised. However, it also asserts that:

> [I]f harm cannot be, by nature, cured even by the self-cleansing mechanism of civil society or if its magnitude is too great to await countervailing ideas and expressions, state intervention is permitted as the primary and freedom of speech and press not protected.[37]

Indeed, illegal content, such as obscene material, falls into an area which government effectively deals with, while harmful content is subject to free speech rights. This viewpoint is similar to the opinion of the European Court of Human Rights which we discussed in the previous section (see Chapter 2.2). However, the Constitutional Court's standard has not been accepted by law enforcement authorities and lower courts (Cho, 2003). Instead, the Supreme Court's three prong test in the *Happy Sara* case — whether it stimulates sexual desires for no special reason; whether it affronts an average person's proper sense of shame about sex; and whether it violates the sound morality on sex — has been applied to a number of cases which contest obscenity.[38] As Professor Cho criticises these standards of obscenity for being moralistic, Professor Moon (2003) also argues that under the standards "even the slightest form of sexual expression could be prohibited," (p. 371) because while its definition of obscenity regards "social value as only one factor that mitigates prurient interest," (p.372) it heavily depends on "the definition of shame and the abstract notion of sound sexual morality." (p. 373)

---

[37] *Ibid.*

[38] see Judgment of August 23, 2002, 2002Do 2889, DAEBEOPWON [Supreme Court]; Judgment of December 22, 2000, 2000Do4372, DAEBEOPWON; Judgment of October 27, 98Do679, DAEBEOPWON (see Chpater2: Footnote 30); Judgment of August 22, 1997, 97Do937, DAEBEOPWON.

In South Korea the court has established substantial jurisprudences concerning obscenity despite the vague provisions of various statutes which regulate obscene materials. However, as discussed, the court's definition of obscenity is still subject to many criticisms, since a number of literary and art works have been classified as obscene material by the court. Furthermore, the Korean court asserts that a judge must take the responsibility of a final decision of whether a speech or expression is obscene, and s/he does not need to go through a procedure of asking other people's opinions.[39] As South Korea has not adopted a jury system, it is questionable whether a judge alone represents an average person's sexual morality and sense of shame about sex (Jong S. Kim, 2003).

Why does the Korean judiciary apply public morality to obscenity cases as a supreme standard? Professor Moon (2003, pp. 380-383) associates it with the paternalism of South Korean society. Professor Cho (2003, pp. 148-149) interprets it as a reflection of a conservative Confucian sexual concept or a puritanical notion about sex. In this context, we may need to recall that D.H. Lawrence's *Lady Chatterley's Lover* and James Joyce's *Ulysses* were once considered to be obscene materials; the definition of potentially harmful content clearly alters over time.

2.6. Governmental Internet Content Regulation

Despite the difficulties of Internet content regulation, the rapid growth of the Internet has led to many governments attempting to regulate it. The most widespread justification for Internet content regulation is the protection of minors from harmful information on the Internet, although some of the more authoritarian governments have introduced Internet content regulations

[39] Judgment February 10, 1995, 94Do2266, DAEBEOPWON [Supreme Court].

primarily for political reasons. However, most of their attempts have instantly faced strong challenges. Many cyber-libertarian organisations and institutions have raised vociferous objections to governmental Internet content regulation. They have argued that governmental Internet content regulation would lead to heavy-handed governmental intervention and eventually violate freedom of thought and expression on the Internet. I will explore these issues in the next subsection, focusing on governmental Internet content regulations in the US, Australia, China, the UK and the EU.

The reason for choosing these nations is that they form a striking contrast to each other in terms of Internet content regulation. Firstly, I will discuss two US legal cases, *the Communications Decency Act* (CDA) 1996 and *the Child Online Protection Act* (COPA) 1998, which attempted to regulate indecency and harmful Internet content with criminal provisions. Secondly, I will explore the Australian government's Internet content regulation which recognises the Internet as a broadcast-like medium. Thirdly, I will consider the Chinese government's authoritative regulatory approach to Internet content regulation. Fourthly, I will discuss the UK and the European Union's co-operative regulatory approach to illegal and harmful content on the Internet. A comparative analysis of their Internet content regulations will be made followed by case studies.

2.6.1. The US

I chose the US as my case study because the US is still dominant in terms of both infrastructure and content on the Internet (see Chapter 2: Footnote 20), and therefore its Internet policy would influence other countries worldwide. The impact of one nation's Internet content regulation would not be limited to a single jurisdiction, but would reach worldwide, because of the global nature of

the Internet (Seo, 2003, p. 7). It has set significant precedents which have extensively interpreted the characteristics of the Internet. These precedents gave rise to heated debates between civil liberty organisations and the government and were eventually brought before the US Supreme Court. They have become seminal in terms of debating Internet content regulation worldwide.

Here, two cases will be discussed from a historical point of view; *the Communication Decency Act* (CDA) and *the Child Online Protection Act* (COPA). The following analysis will begin with discussions about Marty Rimm's study which raised controversy over cyber-porn. I will then trace the detailed procedures of the two lawsuits in order to present a clear picture of the debate over governmental Internet content regulation and freedom of expression.

2.6.1.1. The Communications Decency Act 1996

In February 1995, *the Communications Decency Act* (CDA) was introduced by Senators James Exon (Democrat, Nebraska) and Slade Gorton (Republican, Washington). The proposal subjected individuals to punishment with up to a 100,000 USD fine or 2 years in prison for any "obscene, lewd, lascivious, filthy, or indecent" message transmitted over a telecommunications network to a minor or with intention to "annoy, abuse, threaten or harass." Moreover, it made information providers liable if they were aware of the transmission or if they did not make a reasonable effort to prevent minors from accessing the material.

Ironically, neither Exon nor Gorton had much experience of the Internet and their view of the Internet seemed to be very narrow. They regarded the whole

Internet simply as a haven of debauchery for pornography (Wallace & Mangan, 1997b, p. 173). During 1994, the first year of Exon's campaign for the CDA, not everybody agreed with his opinion, because the CDA radically violated free speech rights that were protected by the First Amendment. However, the situation rapidly changed when the magazine, *TIME*, issued *On a Screen Near You: Cyberporn* as a cover story on 3rd July 1995.

.

The article written by senior *TIME* writer, Philip Elmer-Dewit, exclusively reported Marty Rimm's *Georgetown Law Journal* article, *Marketing Pornography on the Information Superhighway* which has a shocking subtitle, *A Survey of 917,410 Images, Descriptions, Short Stories and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces and Territories*. *TIME*'s article said, "There's an awful lot of porn on-line," and summarised Rimm's study in that pornography on the Internet is "immensely popluar", "a big moneymaker", "ubiquitous", and "not just naked women." (Elmer-Dewitt, 1995).

TIME's cover story and Rimm's study created a sensation and reinforced the position of people who supported restrictions on the Internet. However, his study faced severe critiques as soon as it was published. Hoffman and Novak (1995) criticised Rimm's study for its "misrepresentation, manipulation, lack of objectivity, and methodological flaws." They argued that Rimm's study would mislead the majority of casual readers, since the study was based only on selected adult Bulletin Board Systems in the US, not on the general Internet. They also criticised Rimm for making numerous sensational statements without objective evidence. For instance, Rimm stated that the 917,410 pornographic items were downloaded 8.5 million times. However, he failed to "specify the period of time in which the 8.5 million downloaded accumulated." What is worse, Rimm (1995), made mysterious statistical statements such as:

> 71%, or 1671 of the 2534 pornographic images [were] downloaded from the five UseNet newsgroups [...] (p. 1874). 83.5% of all images posted on the UseNet are pornographic (p. 1914).

Against these statements, Hoffman and Novak pointed out:

> Rimm [did] not provide a listing of the names of these groups, no distributions of posts in these groups, and no methodological discussion of how he counted and determined posts were either pornographic or not, so there is no objective evidence of whether these groups are, in fact, pornographic.

Moreover, Rimm was dishonest. Rimm claimed that the BBS system operators assisted him in the study, although "none of them remember ever having spoken to Rimm or a member of his research team about the study." (Meeks, 1995) Rimm also insisted that the study was produced by a research team which consisted of "more than two dozen faculty, staff, graduate and undergraduate students at Carnegie Mellon University." (Rimm, 1995, p. 1861) *TIME*'s article introduced Rimm as a principal investigator, however this was not true at all. Indeed, the study was conducted solely by the author, Rimm. Just after the article published, Provost of Carnegie Mellon University, Paul Christiano, issued a press release which stated, "the study was the individual work of undergraduate Marty Rimm and should not be referred to as the Carnegie Mellon study." (Wallace & Mangan, 1997b, p. 150) The Senate cancelled its plan of calling Rimm as a witness on the hearing concerning Internet pornography (p. 151). However, even after the sensation had subsided, Rimm's influence remained. The voice of people who wanted to restrict the Internet became louder and they used his study as a tool for witch-hunting on the Internet.

On 8th February 1996, the bill was finally signed into law by President Clinton.

The CDA, which is the first law for protecting minors from pornographic Internet material in the US, became part of *the Telecommunications Reform Bill.*

However, ironically, on the same day, the American Civil Liberties Union (ACLU) and other civil organisations filed a suit in Philadelphia. About two weeks later, on 26th Februray, a second lawsuit, *American Library Association v. Reno*, was filed in the same federal district court in Philadelphia and was consolidated with the first suit, *ACLU v. Reno*. The plaintiffs insisted that two sections of the CDA, section 223 (a) and (d),[40] violated the First Amendment, and claimed a preliminary injunction. Many citizens on the Internet proved to be the strongest supporters of free speech rights. The day on which the CDA was passed by Congress was named 'Black Thursday.' Many Websites including Yahoo, one of the biggest search engines on the Internet, turned their pages black for 48 hours in support of the coalition to stop the CDA.[41] Wallace and Mangan (1997a), the co-authors of *Sex, Laws, and Cyberspace*, argued that the CDA criminalised 'indecent' speech on the Internet while it is legitimate in

---

[40] According to the *ACLU v. Reno* decision of the Federal District Court of Philadelphia (929 F. Supp. 824):

> Section 223(a)(1)(B) provides in part that any person in interstate or foreign communications who, "by means of a telecommunications device," (5) "knowingly [...] makes, creates, or solicits" and "initiates the transmission" of "any comment, request, suggestion, proposal, image or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age," "shall be criminally fined or imprisoned."
>
> Section 223(d)(1) ("the patently offensive provision"), makes it a crime to use an "interactive computer service"(6) to "send" or "display in a manner available" to a person under age 18, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication."

[41] The Yahoo!'s black page is available at http://mirrors.yahoo.com/eff/speech.html (Retrieved March 21, 2001)

print media.[42]

Since in the US indecency laws cannot be applied to print media, while broadcast media such as television and radio are covered by the laws, the question of whether the Internet is print or broadcast medium was one of the key issues addressed in the CDA case. The plaintiffs of the CDA case claimed that the Internet should enjoy freedom of expression just like print media and should not be regulated in the way broadcast media is regulated. They also argued that when people explore the Internet it is the same as if they were in a library. In a sense, the Internet is a print medium. It uses communication tools only for accessing. Books, magazines and other printed material must physically be brought into our homes, so they are considered 'invited' and cannot be censored. People invite information into their home through the Internet. Thus, the information available on the Internet would be treated like the information available in books and magazines, not like broadcast media — The Internet has strengthened its characteristics as a broadcast medium. VOD (Video-On-Demand) and Streaming services on the Internet are such examples. However, it does not necessarily mean that the Internet is a broadcast medium. The Internet is a truly complex medium that has integrated all kinds of human communication technologies into itself. Flint (2000) argues that even if an Internet service passes the 'look and feel' test of broadcasting, it is not broadcasting, unless the service uses the broadcasting services bands, such as the radio frequency spectrum. Kim Yi-Gi (2002) also discussed that the Streaming service cannot be treated as a broadcast medium, because it does not use the radio spectrum which is a public resource, and therefore regulatory

[42] In the US, while broadcast is subject to indecency laws, they are unconstitutional as applied to print media. The Supreme Court case, *Butler v. Michigan* (352U.S.380, 1957) is a prime example. The Supreme Court held a Michigan law as unconstitutional, which made criminal the sale of books that might have a bad effect on young people (Wallace & Mangan, 1997b, p. 30).

principle of a scarcity of usable frequencies in the radio spectrum[43] which has been a ground of strict governmental regulation on broadcasting cannot be applied to it (see Chapter 2.7).

Another serious problem addressed by the CDA was its use of the 'contemporary community standard.' [44] First of all, the notion of 'contemporary community standards' is extremely ambiguous, not to say absurd, given that the US is a plural and diverse society. For instance, a book may be obscene in Tennessee, but legal in New York. Therefore, if the vague community standard of the CDA is applied, any material placed on the Internet must satisfy the standards of every community anywhere in the US.

On 12th June 1996, a three-judge panel in the Federal District Court of Philadelphia held that the CDA was unconstitutional. The Court held that the Internet is not an invasive broadcast medium in its finding of facts, because "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial" on radio or television (*ACLU v. Reno* 929 F. Supp. 824, 1996, Finding of Fact [88] and [98]). In the decision, District Judge Stewart Dalzell significantly defined the Internet as "a never-ending worldwide conversation" and "the most participatory form of

---

[43] In 1969 the US Supreme Court clarified that "broadcast frequencies constituted a scarce resource" in the case of *Red Lion Broadcasting Co., Inc. v. Federal Communications Commission (FCC)* [395 U.S. 367(1969)].

[44] The community standard is one of measures of the so-called Miller test. In a case called *Miller v. California* (413U.S.15, 1973) the US Supreme Court announced the three-part test to identify obscene speech. To be obscene a speech or material must meet all three parts of the test below:

> (a) whether "the average person, applying contemporary community standards" would find that the work, taken as a whole, appeals to the prurient interest, [...] (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

mass speech." Therefore he asserted, "[T]he Internet deserves the highest protection from governmental intrusion." (*ACLU v. Reno* 929 F. Supp. 824, 1996).

A year after the Federal District Court's decision, the CDA was finally rejected. On Thursday June 26, 1997, the US Supreme Court ruled the CDA unconstitutional for the reason that "indecent transmission" and "patently offensive display" provisions of the CDA restrict "the freedom of speech" which is protected by the First Amendment (*ACLU v. Reno* 512U.S. No.96-511).[45]

This was the first regulatory attempt of the US government over Internet contents. The US Court's decision, which recognised the Internet as a print-like medium and as "the most participatory" medium, became a milestone over Internet content regulation worldwide. Akdeniz (1999, p. 29) appraised that it was "an important step for freedom of speech on the Internet." However, it was not the end of story for the US government's Internet content regulation. In October 1998, another similar bill known as *the Child Online Protection Act* (COPA) was introduced.

2.6.1.2. The Child Online Protection Act 1998

The COPA was passed by Congress and signed into law by President Clinton in 1998. The chief sponsor of this bill was Senator Dan Coats, who was a co-sponsor of the original CDA. The COPA was colloquially referred to as 'CDA II' and had the same objectives as the CDA which had been ruled

[45] The full text of the Court's decision is available at EPIC's Website, http://www2.epic.org/cda/cda_decision.html (Retrieved May 2, 2003)

unconstitutional. The CDA II made it a federal crime for commercial Websites to communicate material considered 'harmful-to-minors.' Penalties included criminal and civil fines of up to 150,000 USD for each day of violation and up to 6 months in prison if convicted (ACLU, 1999a).

Like the CDA, the CDA II suppressed, even if to a lesser extent, material that was permissible for adults. Its approach used a 'harmful-to-minors' standard rather than the vague indecency standard. The 'harmful-to-minors' standard has been upheld by various courts for more than three decades. In a 1968 case, *Ginsberg v. New York*, the court upheld the constitutionality of a New York law that prohibited selling minors material that was harmful to them but not obscene for adults (Hudson, 1998). Thus, supporters of the CDA II, including the National Law Center for Children and Families,[46] thought it would pass constitutional scrutiny, since this law only applied to people who could comply financially with the adult verification requirements, such as commercial pornographers on the World Wide Web.

However, the CDA II was based on the idea of 'community standards' which were ruled unconstitutional during the legislation process of the CDA. Senator Ron Wyden who opposes the CDA II said, "This is one-size-fits-all." (Wasserman, 1998) Furthermore, the 'harmful-to-minors' standard still remains as a vague standard on the Internet. Opponents, such as the ACLU and the Electronic Frontier Foundation (EFF), insisted that it could have a deleterious effect in unintended ways on electronic commerce, as well as on the dissemination of free speech online. Although the CDA II targeted

[46] The National Law Center for Children and Families (NLC) is a non-profit organisation which is based on Fairfax, Virginia US. It focuses on the protection of children and families from the harmful effect of illegal pornography by assisting law enforcement and law improvement (Resource: NLC Website. Retrieved May 2, 2003, from http://www.nationallawcenter.org).

commercial Websites, the term, 'harmful-to-minors' is "so broad that it covers anything from an online bookseller like Amazon.com to a non-profit Website that sells books or T-shirts." (Internet Free Expression Alliance, 1998)

On 22nd October 1998, seventeen organisations challenged the Act, known as *ACLU v. Reno II.* The seventeen plaintiffs in the challenge included the Electronic Privacy Information Centre (EPIC), the EFF, and the ACLU which led the unconstitutional judgment of the CDA through the case, *ACLU v. Reno* (ACLU, 1999b). On 1st February 1999, the US Federal District judge halted enforcement of the CDA II. The Judge, Lowell A. Reed, Jr., accepted some of the plaintiffs' claim that the federal Internet censorship law violates the First Amendment rights of adults and issued a preliminary injunction against the CDA II.[47]

In May 2002, the Supreme Court issued a decision on the COPA.[48] The Court sent the case back to the appeals court and ordered the lower court to decide the case on a wider range of First Amendment issues. The Court also left in place an injunction barring enforcement of the law. Finally, on 6th May 2003, the Federal Court, the Third Circuit Court of Appeals, ruled that the COPA was unconstitutional. The Court found that it violated the First Amendment because it improperly restricted access to a substantial amount of online speech that was lawful for adults.[49]

---

[47] The full text of the Court's decision is available on the EPIC Website at http://www.epic.org/free_speech/copa/pi_decision.html (Retrieved May 2, 2003)

[48] The Supreme Court's decision is available at http://www.supremecourtus.gov/opinions/01pdf/00-1293.pdf (Retrieved May 3, 2003)

[49] The Court's decision is available at http://caselaw.lp.findlaw.com/data2/circs/3rd/991324p.pdf (Retrieved May 3, 2003)

2.6.1.3. The Implications of the CDA and the COPA

In my view, the first significant outcome of the CDA case is that the Court held that indecent or potentially harmful content on the Internet falls within the protection area of freedom of expression and therefore cannot be subject to a criminal provision. As discussed above, harmful content is a different issue from illegal content. It requires a separate regulatory approach from illegal content. It is unfair to entirely prohibit indecent material on the Internet, while the same material is legally protected in other media. Professor Cho (2003) argues that criminal law should only be applied to obscene material, not to indecent material.

The second significant outcome of the CDA case is that the Court defines the Internet as a medium which is similar to print media, rather than as a broadcast medium. The Internet is providing a wide range of communication and information services which various traditional media used to provide so it is difficult to classify the Internet under one of the existing medium categories. Moreover, the advent of broadband service has strengthened its characteristics as an interactive broadcast medium. However, the mechanism of broadcast service on the Internet is completely different from the way of existing broadcast services because it does not permeate into every household but end-users can enjoy it only when they specifically request it. Esther Dyson (1998, pp. 208-209) argued that:

> [On the Internet] content that is accessible must be sought out and downloaded or visited; except for e-mail, it doesn't come at you unbidden. You have to *join* discussion groups, whether through mailing lists, Websites, or chats – some restricted, some open to anyone. You must *sign up* for the new proliferating "push" services that send you stuff automatically. You have to *act purposely* to get to

all these things; they don't grab you.

In this sense, it can be said that the Internet cannot be regulated as a broadcasting medium, but it can be treated as a print medium, in order to maintain its current state.

In sum, the US government's regulatory attempts on Internet content were undermined by the US Supreme Court which is traditionally in favour of freedom of expression. The Court's decision has influenced many cyber-libertarians worldwide. For instance, in 2002 the Korean Constitutional Court ruled that the Korean government's Internet regulation was unconstitutional (99Hun-Ma480, 14-1 KCC 616), largely on the basis of legal opinion which the US Supreme Court announced in connection with the CDA case (see Chapter 9.2).

Despite the failure of the two previous legislations, in December 2000 the US President Clinton signed another Internet content regulation, *the Children's Internet Protection Act* (CIPA), into law. However, the CIPA is less restrictive compared to the previous two regulations. It applies only to public libraries and schools. It does not target general Internet contents nor impose any punitive penalties – the CIPA has also introduced a contentious debate concerning free speech rights on the Internet. I will discuss the CIPA in Chapter 4 in depth.

Since then, the main stream of Internet content regulation in the US has turned towards self-regulation of the civil and industrial sectors. In July 1997, a report from the Clinton Administration, *the Framework for Global Electronic Commerce*, emphasised the private sector's role in the development of the Internet. In particular, as regards Internet content regulation, the report supported "industry self-regulation, adopting of competing rating system, and

development of easy-to-use technical solutions," such as filtering technologies and age verification systems. (White House, 1997) This trend led to the development of Internet content rating systems, such as SafeSurf and RSACi. It resulted in a significant growth of the commercial Internet content filtering software market. Internet filtering software and Internet content rating systems will be discussed in Chapters 4 and 5 respectively.

2.6.2. Australia

The Australian government's regulatory approach to Internet content forms a clear contrast to the US. Firstly, for dealing with illegal and harmful Internet content it has employed a co-operative regulatory model. Secondly, while the US Court found that the Internet is not an invasive broadcast medium, in Australia, Internet content is regulated by the Australian Broadcasting Authority (ABA) and the Office of Film and Literature Classification (OFLC). In the following section, *the Broadcasting Services Amendment (Online Services) Act 1999* (BSA)[50] which has been a foundation for regulating Internet content in Australia will be discussed. Furthermore, the merits and demerits of the Australian government's Internet content regulation will be considered.

2.6.2.1. The Broadcasting Services Amendment (Online Services) Act 1999

In June 1999 the Australian Commonwealth government introduced Internet content legislation, *the Broadcasting Services Amendment (Online Services) Act 1999* (BSA), which came into effect on 1st January 2000. The main

[50] The full text of the BSA 1999 is available on the Parliament of Australia Website at http://www.aph.gov.au/parlinfo/billsnet/99077.pdf (Retrieved February 21, 2005).

elements of the Act are: establishing a complaints mechanism, categorising Internet content, empowering the ABA, and providing indemnities for Internet service providers. To comply with the Act the ABA implemented a complaints system enabling members of the public,[51] so-called an Internet hotline, to make complaints to the ABA about Internet content which is, or may be, prohibited by law. They can make a complaint by completing the online complaint form. Alternatively, the form can be posted to the ABA. After that, the general procedure followed for the complaints system is as follows:

> [If] the content is hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will direct the Internet content host to remove the content from their service. If the content is not hosted in Australia and is prohibited, or is likely to be prohibited, the ABA will notify the content to the suppliers of approved filters in accordance with the Internet Industry Association's code of practice. If the content is also sufficiently serious (for example, illegal material such as child pornography), the ABA may refer the material to the appropriate law enforcement agency (Minister for Communications, Information Technology and the Arts, 2000, p. 8).

The Act defines Internet content as information that is "kept on a data storage device and is accessed, or available for access, using an Internet carriage service,"[52] including material on the Web, postings on newsgroups and bulletin boards, and other files that can be downloaded from an archive or library. However, it does not include "ordinary electronic mail or information that is transmitted in the form of a broadcasting service" that is accessed in real time without being previously stored, such as chat services and voice over the

---

[51] According to the ABA, to make a complaint about Internet content, someone must be one of the following: an Australian resident or a corporate body that carries on activities in Australia or the Commonwealth, a state or a territory (BSA, Section 25 – Residency etc. of Complainant).

[52] The BSA, Schedule 5—Online services, Part 1—Introduction, 3. Definitions.

Internet.

In accordance with the Act, the OFLC classifies Internet content according to the National Classification guidelines. Internet sites hosted in Australia that contain 'Restricted'-rated information must provide restricted access systems which verify adult status, while Internet content which is classified into 'RC (Refused Classification)' or 'X' is prohibited. The RC category includes material containing detailed instruction in crime, violence or drug use, child pornography, bestiality, real depictions of actual sexual activity and excessively violent or sexually violent material (OFLC, 1999).

In September 1999, Australia's national Internet industry organisation, the Internet Industry Association (IIA), released its Code of Practice (Draft Version 5.0) which included sections designed to comply with the BSA, in particular, Clause 60 of the BSA —'Matters that must be dealt with by industry codes and industry standards.'[53] Under Article 12A.4[54] of the Code of Practice (version 5.0) Internet service providers (ISPs) are required to provide

---

[53] This provision articulates that an industry code or an industry standard should deals with "alternative access-prevention arrangements" for end-users, including Internet content filtering software and family-friendly filtered Internet carriage service.

[54] Article 12A.4 of the Code is as follows:

> ISPs will take reasonable steps to provide users with information about:
>
> (a) supervising and controlling children's access to Internet content; (b) procedures which parents can implement to control children's access to Internet content, including the availability, use and appropriate application of Internet Content filtering software; (c) their legal responsibilities, as they may exist under the *Broadcasting Services Act* 1992 or corresponding State legislation in relation to Content which they intend to provide to the public via the Internet from within Australia.
>
> ISPs shall be taken to have fulfilled these requirements to the extent that they direct users, by means of a link on their Home Page or otherwise, to resources made available for the purpose from time to time by the Administration Council, the IIA, the ABA or Netwatch.

Internet content filtering software to their users. In December 1999 the ABA approved 'Internet Industry Codes of Practice' (version 6.0) (Internet Industry Association, 1999).[55] This version included a list of Internet content filtering products and services which Internet service providers within Australia are required to "provide for use, at a charge determined by the ISPs."[56]

Alongside these legislative measures, the Australian government has also launched an awareness and education campaign for Internet safety. In 1999 the government established the NetAlert, an Internet safety advisory body, to educate communities about managing access to online content. It has also undertaken a range of activities to provide information about ways of addressing illegal and harmful content, such as providing a toll-free help line, distributing the NetAlert information kit and holding forums across Australia (Minister for Communications, Information Technology and the Arts, 2001; 2002).[57]

2.6.2.2. The Features of the Australian Internet Content Regulation

In my view, the most significant feature of the Australian government's Internet regulation is that it formed the driving force behind the Internet industry's regulatory efforts, such as introducing industrial codes of conduct. It has provided a complaints system to report illegal content by Internet end-users

---

[55] The Code was last updated in May 2002 (version 7.2).

[56] Clause 6.2 (a) of the Code (version 6.0) is as follows:

> ISPs who provide Internet access to subscribers within Australia will as soon as reasonably practicable for each person who subscribes to an ISP's Internet carriage service provide for use, at a charge determined by the ISP [...].

[57] More information about the NetAlert is available on its Website at http://www.netalert.net.au/ (Retrieved March 5, 2003).

and it has also conducted awareness and education campaigns. Thus, the Australian Internet content regulation can be summarised in three elements; self-regulation, hotlines and awareness campaigns. These multi-dimensional regulatory solutions are quite consistent with the UK and the European Union's co-regulatory approach which will be discussed later in this chapter (see Chapter 2.6.4). Since September 2000, the ABA has been a member of the Internet Hotline Providers in Europe Association, INHOPE, which is partly funded by the European Commission (see Chapter 3.6.2). Overall, its regulatory approach to Internet content regulation is obviously much more advanced than the US government's previous Internet regulations; the CDA in 1996 and the COPA in 1998.

2.6.2.3. A Critique of the Australian Internet Content Regulation

However, many libertarians and organisations such as the Electronic Frontiers Australia (EFA)[58] claimed that the BSA is aimed at censorship and its scheme is unworkable. They criticised the Act for inappropriate guidelines for Internet content classification, jurisdiction issues and reliability of filtering software as follows (EFA, 2002b; Taggart, 2001 & Taylor, 2001).

Firstly, because the Australian regulation regime classifies Internet content using guidelines for films and videos which are more restrictive than guidelines for publications, it is possible that certain prohibited Internet material under the Act is legally available in other media, such as books and magazines. As a result, freedom of expression on the Internet may be restricted by the Act.

[58] The EFA was formed in January 1994 and incorporated under South Australian law in May 1994. It is a non-profit national organisation representing Internet users concerned with on-line freedoms and rights.

Secondly, as mentioned above, much information on the Internet comes from outside jurisdiction. Although the ABA has power to direct Internet content hosts in Australia to remove prohibited content from their servers, there is little that the ABA can do about content hosted overseas. According to the *Six-Months Report on Co-Regulatory Scheme for Internet Content Regulation: July to December 2000* (Minister for Communications, Information Technology and the Arts, 2001) in the course of six months, of 139 complaints which were determined to relate to prohibited content, only six were found to be hosted in Australia. This trend has not changed over the last few years. According to *the ABA Annual Report 2003-2004* (ABA, 2004), of 708 prohibited or potentially prohibited items which the ABA found, only seven items were hosted in Australia, while 701 items were found to be hosted outside Australia during the reporting period.

Thirdly, the effectiveness of the Internet content filtering products and services which are approved by the ABA is very doubtful, since these kinds of products and services have been heavily criticised for seriously affecting individual freedoms. Civil organisations, such as the ACLU and the American Library Association (ALA), have argued that commercial filtering products block not only illegal Internet materials, but also controversial and innocent materials, while they frequently omit to block some potentially harmful information on the Internet. Moreover, their failings cannot be eradicated, but are inherent – in Chapter 4 issues concerning the Internet content filtering technologies and commercial products will be discussed in depth. In my view, the use of Internet content filtering software is a matter of user choice. It would not be recommended that a governmental agency gives commercial filtering software credit.

Despite these criticisms, the Australian government said that:

> Claims that the [...] legislation is aimed at censorship are completely untrue. It merely applies to the Internet the same classification systems as apply to other forms of media. [...] The new scheme strikes an appropriate balance between community concerns about illegal and offensive online content and the interests of industry and all Internet users. It reflects moves by the Government and the Australian Internet industry to help protect Australian citizens, especially children, from illegal or highly offensive material on the Internet (McGauran, 2000).

Nevertheless, the Australian government's Internet regulation is still problematic. Heins (2001, p. 226) criticises the Australian Internet industry's self-regulation because it has not been free of official involvement from the very beginning. It is simply impracticable to classify vast amounts of information on the Internet which are largely hosted outside Australia under the Australian government's National Classification guidelines for films. Indeed, in my view, one of the most controversial issues is that it categories the Internet as a broadcast medium. Therefore, it applies relatively restrictive standards of public broadcast media to the Internet. Furthermore, this case study also reveals that the Australian government's complaints system has quite limited effects. In sum, the existence of the super-empowered ABA remains highly controversial. It seems to overwhelm the government's efforts to encourage the industry's self-regulatory efforts.

2.6.3. China

The next country that I will consider is China. It remains a largely authoritarian state rather than a democracy so it provides an interesting contrast to Western democracies. While many Western governments have introduced Internet regulations mainly aimed at dealing with obscene and pornographic material on the Internet, the Chinese government has a serious concern about uncontrolled information through the Internet which may undermine its sovereignty and

social order, as well as cultural values. In this sense, Internet regulation in China is based on the idea that the government should monitor and control information on the Internet.

The Chinese government has employed two different types of regulatory approaches to the Internet. The first solution is based on direct governmental regulation, including promulgation of a series of legislative acts. Another solution adopts the new information technologies, such as filtering and surveillance tools. In this section I will discuss the Chinese government's Internet-related legislation during the period of 1996-2000. Furthermore, the technical means of censorship which have been employed by the Chinese government will be considered.

2.6.3.1. China: Internet Legislation 1996-2000

Since the Internet was first made available to the general public in China in 1995, a number of regulations have been issued in order to control and monitor Internet content. In February 1996 the Chinese government promulgated an Internet regulation which is named *People's Republic of China Interim Regulations Governing the Management of International Computer Networks*. [59] The law contains a number of controversial provisions. Particularly, Article 6 of the law reads:

> Computer information networks conducting direct international networking shall use the international access channels provided by the national public telecommunications networks of the Ministry of Posts and Telecommunications. No units or individuals shall set up by

[59] The full text of the law is available in English via the Website of the China Law Society at the University of Maryland, US, http://www.qis.net/chinalaw/index.html (Retrieved March 11, 2004)

themselves or use other access channels for international networking.

Then, Article 13 states:

> Units and individuals engaging in international networking [...] are not allowed to use international networking to harm national security, leak state secrets, and engage in law-breaking criminal activities; and they are not allowed to produce, read, duplicate, or circulate information hampering public security and obscene pornographic information.

The Chinese government revised its Internet regulation in December 1997. The new regulation which is called *the Computer Information Network and Internet Security, Protection and Management Regulations*[60] was approved by the State Council on 11th December 1997 and promulgated by the Ministry of Public Security on 30th December 1997. The new regulation aimed at managing and controlling the security of domestic and international computer information network connections. It described the duties and responsibilities of China's Internet service providers and users. Article 5 of the law stated:

> No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information: (1) Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations; (2) Inciting to overthrow the government or the socialist system; (3) Inciting division of the country, harming national unification; (4) Inciting hatred or discrimination among nationalities or harming the unity of the nationalities; (5) Making falsehoods or distorting the truth, spreading rumors, destroying the order of society; (6) Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder, (7) Terrorism or inciting others to criminal activity; openly insulting other people or

[60] The full text of the law is available in English at http://www.chinaonline.com/refer/legal/laws_regs/pdf/c00012670e.pdf (Retrieved January 17, 2002)

distorting the truth to slander people; (8) Injuring the reputation of state organs; (9) Other activities against the Constitution, laws or administrative regulations.

In September 2000 the State Council issued a more stringent Internet regulation, *the Measures for Managing the Internet Information Services*.[61] Article 14 says that an ISP must record information of its subscribers' online activities and must keep a copy of their records for 60 days. ISPs are obliged to furnish them to the relevant state authorities upon demand in accordance with the law.

In sum, the Chinese government has introduced a number of criminal provisions which tightly regulate Internet content and usage. In particular, throughout the legislation, the government repeatedly emphasised the responsibilities of individual Internet users and Internet service providers for preventing antisocial or political dissident activities on the Internet. As mentioned above, it articulates a list of illegal Internet information and activities without drawing a distinction between illegal and harmful content.

2.6.3.2. Technical Measures for Controlling Internet Content in China

Apart from strict regulations, the Chinese government has officially employed a number of technical measures in order to control information on the Internet, such as monitoring and filtering Websites and e-mail addresses. Indeed, in my view, China is the country which has adopted the most extensive and sophisticated technical censorship measures on the Internet.

---

[61] The full text of the law is available in English at http://www.chinaonline.com/issues/internet_policy/regulations/c9091709.asp (Retrieved April 14, 2004)

The Chinese government has blocked a few dozen foreign Websites at several major Internet entry points, such as ChinaNet. In June 1995, only a few months after the Chinese government started to offer commercial access to the Internet, the Minister of Post and Telecommunications, Wu Jichuan, had already reaffirmed that China was committed as a sovereign state to monitoring the information flowing into the country (Sautede, 1996). This is the so-called 'digital Great Wall' which is officially known as a 'firewall' and is designed to keep Chinese cyberspace free of objectionable materials of all sorts. The digital Great Wall does not need great technical know-how, because "[Internet] connections to the outside world are required to pass through a handful of official gateways" (Barme & Ye, 1997) under the regulations. The Chinese censorship system involves blocking "access IP addresses, surveillance of users, the use of informers, arrest and seizures." (Rodriquez, 2003) Another implementation of Chinese Internet censorship is the so-called DNS (Domain Name Server) hijacking. Zittrain and Edelman (2003), through their *Empirical Analysis of Internet in China*, confirm, "DNS servers in China report a Web server other than the official Web server actually designated via each site's authoritative name servers."

> [...] the IP address 64.33.88.161. That IP address is associated with the host www.falundafa.ca, the site of a Canadian organisation that promotes the practice of Falun Gong. However, that address is itself blocked by Chinese border routers, preventing such requests from reaching either the falundafa server or any other. As a result, Chinese users are unable to reach the entirety of these many sites, including their respective default pages as well as their subsidiary pages (Zittrain & Edelman, 2003).

Filtering on the basis of IP address is difficult to circumvent, although there is a common circumvention method which "relies on channeling Webpage requests and viewing associated results through proxy servers which are themselves

outside China." In a case of filtering on the basis of DNS, in order to circumvent it, users would simply type the numeric IP address of the desired Web server in their browser's location bar (Zittrain & Edelman, 2003). However, it is not easy to know the server's IP address for most moderate Internet users. It has been frequently reported that most of the Western media, including CNN and the New York Times, are being blocked (Neumann, 2001).

In 2000 the Chinese government launched a broader telecommunications surveillance scheme, the so-called Golden Shield Project, as the fourth phrase of Golden Projects which first started in 1993 for the development of information infrastructure in China (Cullen & Choy, 1999). According to a report by the International Centre for Human Rights and Democratic Development (Walton, 2001), the Golden Shield Project is "a database-driven remote surveillance system" which incorporates speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies. It aims to adopt "advanced information and communication technology to strengthen central police control, responsiveness and crime combating capacity, so as to improve the efficiency and effectiveness of police work."

2.6.3.3. A Modern Paradox in China

In conclusion, while the number of Chinese Internet users has grown explosively[62] and the rapid development of infrastructure has accelerated the

[62] The number of Internet users in People's Republic China.

Jan.1999	Jan. 2000	Jan. 2001	Jan. 2002	Jan. 2003	June 2003
2.1 million	8.9 million	22.5 million	33.7 million	59.1 million	68 million

(Resource: The China Internet Network Information Centre Website. Retrieved April 14, 2004, from http://www.cnnic.net.cn/)

development of the Internet in China,[63] Internet content regulation in China have been tightened up and there is still no sign of change regarding current Internet policies of the Chinese government. On the contrary, President Jiang Zemin called for tighter controls against "pernicious information" being spread online in the fast-growing Chinese Internet market at a central committee meeting of the communist party on 12th July 2001 ("Jiang renews," 2001). In this context, it can be said that the Chinese government's Internet content regulation policy goes against the trend of Western governments' towards minimising their role in Internet content regulation systems, particularly regarding harmful Internet content. According to reports from Human Rights Watch (2001), a number of Chinese Internet users have been detained or imprisoned as a result of posting material which the government deemed to be subversive on the Internet. Walton (2001) says that in China "fighting crime is willfully confused with suppressing dissent."

Although China has its own unique social and political background, which is very different from that of many Western countries, its Internet content regulation interrupts the free flow of a vast amount of healthy information on the Internet and excludes millions of Chinese from the great benefits which the Internet has brought. A report from RAND (Chase & Mulvenon, 2002) says, "China faces a very modern paradox." The report comments that the Internet is a key engine of the new Chinese economy, but at the same time China still fears that an advanced communication infrastructure may jeopardise its social and political security. In the immediate future it may become a serious obstacle to the development of the Internet in China, because it may "frighten off

[63] According to a report from the US Embassy in Beijing (1998), more than 80 percent of China's communication backbone and 40 percent of its urban networks use fibre optic cable. China is one of the first countries outside the US to have started large-scale deployment of digital wave division multiplexing systems. China's national telecommunications system is already second in size to that of the US.

foreign direct investment, undermining China's efforts to exploit the economic potential of the Internet." (International Centre for Human Rights and Democratic Development, 2001)

However, China is not the only country which exercises an extensive and repressive regulatory policy on the Internet. In a report from the International Federation of Library Associations and Institutions (IFLA), *Libraries, Conflicts and the Internet*, Hamilton (2002, pp. 15-30) said that many nations, from Asia and the Middle East to Latin America and Africa, are experiencing "various type of access barriers with regards to Internet-based information." For instance, Burmese, North Korean and Cuban governments have tightly controlled their Internet access. According to Hamilton, "Burma requires all telecommunications devices to be registered with the government under threat of imprisonment." In Cuba "individuals at home are almost never granted Internet access – the government outlawed the sale of PCs to members of the public in March 2002." Indeed, in these countries freedom of access to information and freedom of expression on the Internet seem to be deprived in attempts to maintain their political power structures. To understand these heavy-handed government Internet content regulation policies, we may need to consider them within a wider political context, but this thesis does not cover each nation's socio-political background.

2.6.4. The EU and the UK

As my last case study in this chapter, the Internet content policies in the UK and the EU are considered. I choose the EU because it has played a leading role in regulating illegal and harmful content on the Internet. It presents a significant contrast to the US. While the US government has introduced a series of legislative acts to regulate Internet content (see Chapter 2.6.1), the EU

has developed a multi-layered co-regulation which incorporates governmental law enforcement, self-regulation of the Internet industry, filtering/rating tools and awareness/education campaigns. Aside from its endorsement of self-regulation, the EU also established the major legal frameworks which aim to harmonise national laws against illegal content on the Internet at the European level.

Firstly, the UK case will be considered. The UK government's Internet content policy has been entirely consistent with EU policy in this matter. In this section the UK government's legislation against illegal content, in particular child pornography, will be discussed. This case study focuses on how national laws have been amended to cover the issues of the Internet era. Secondly, the development of the EU Internet content policy will be explored.

2.6.4.1. The UK: Governmental Regulation against Obscene Internet Content

The UK government has enforced a number of laws to deal with obscene materials on the Internet. In England and Wales the two statutes, *the Obscene Publication Act* (OPA) 1959 and 1964, have provided legal ground to govern all pornography. Section 1(1) of the OPA 1959 articulates the test of obscenity:

> [A]n article shall be deemed to be obscene if its effect or [...] the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

According to Section 1(2) of the Act, the meaning of "article" is "any description of article containing or embodying matter to be read or looked at or

both, any sound record, and any film or other record of a picture or pictures." Section 1(3) adds that "article" includes material in electronic data format. Any kind of digital data storage, such as a computer disk or a CD-ROM can be an article. This Section did not initially include a material in digital formats, however, it was amended by *the Criminal Justice and Public Order Act* (CJPOA) 1994. The CJPOA 1994 added the words: "or, where the matter is data stored electronically, transmits that data." This amendment was introduced to cover the electronic transmission of pornographic material between computers using a modem or a telephone line. Thus, "When A sends B pornographic pictures attached to an-email, this electronic transmission will be a publication covered by the Act." (Akdeniz, 1996, p.237) Furthermore, Section 1(2) of the OPA 1964 makes it an offence "to have an article for publication for gain if with a view to such publication he has the article in his ownership, possession or control."

In response to a growing problem of child pornography and concern about its potential links with paedophilia, *the Protection of Children Act* (PCA) was passed in 1978 (Gibbons, 1995, p.87). Similar to the case of the OPA, the definition of "photograph" in the PCA 1978 was also amended by the CJPOA 1994. Therefore, the meaning of "photograph" in the PCA 1978 includes "data stored on a computer disc or by other electronic means which is capable of conversion into a photograph"[64] and "pseudo-photographs."[65] Again, as

[64] Section 7(4)(b) of the PCA 1978. The extended meaning of "publication" by the CJPOA 1994 became an issue in the *R. v. Fellows* and *R. v. Arnold* case (1996, September 27. *All England Law Reports*, 1997(2), 548-560; *Court of Appeal Reports*, 1997(1), 244-256; Criminal Law Review, 1997, 524-526). Alban Fellows had used his computer to store indecent pictures of children to display on the computer screen and to print them. He also made the data available on the Internet, but the data could only be accessed by those to whom a password was given. Stephen Arnold was a computer user who received the password on contributing similar data to the archive. They were sentenced to three years' and six months' imprisonment respectively at the trial court. In September 1996, the court of appeal dismissed their appeal. Manchester (1996, p. 646) claims that this case is significant in that the court showed that the

regards child pornography, Section 84(4) of the CJPOA 1994 amended Section 160 of the Criminal Justice Act (CJA) 1988 to made it an offence for a person "to have any indecent photograph or pseudo-photograph of a child in his possession."[66] This amendment shows how seriously the UK government takes the issues relating to child pornography. Neither the PCA 1978 nor the OPA 1959 made the simple possession of an obscene article illegal. It is not an offence to possess any other obscene article, apart from child pornography (House of Commons, Home Affairs Committee, 1994, p. vi-vii). Under Section 160 of the CJA 1988, a number of people have been successfully prosecuted for possessing indecent photographs of children (Akdeniz, 1997b; 2003).

As discussed above, the UK government has made an effort to address problems which have emerged from the Internet through a number of legislative changes. However, at the same time, the government has been concerned about the effectiveness of law enforcement. The House of Lords, Select Committee on Science and Technology (1996, para. 4.162) states that the Internet's global character means that the impact of legislation is difficult to predict. Indeed, the UK government does not say that legislation is the answer for all of the issues concerning Internet content. Aside from its law enforcement against illegal Internet content, the UK government has preferred

---

definition of photograph in the PCA 1978 can extend to intangible objects which are capable of replicating a photograph.

[65] Section 84 of the CJPOA 1994 introduced the concept of "pseudo-photographs of children." Section 7(7) of the PCA 1978 defines it as "an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph." Akdeniz (1997b) defined that:

> Pesudo-photographs are technically photographs, but they are created by computer software [...] by using more than one picture. For example a child's face can be superimposed on an adult body or to another child's body together with the alternation of the characteristics of the body to create computer generated images where no physical abuse of a child occurs.

[66] Section 160(1) of the CJA 1988.

self-regulatory approaches to Internet content regulation. The Select Committee on Science and Technology stated, "The best hope of controlling the circulation of undesirable material on the Internet is self-regulation." (House of Lords, Select Committee on Science and Technology, 1996, para, 5.50) During the last decade, a few Internet self-regulatory institutions, such as the Internet Watch Foundation (see Chapter 3.6.1), have been established and played an important role in Internet content regulation in the UK. The Internet self-regulatory policy and organisations in the UK will be discussed further in Chapter 3.

2.6.4.2. The Development of the EU Internet Content Policy

In 1996, while the CDA was introduced in a moral panic in the US (see Chapter 2.6.1), Europe took a very different approach to regulating the Internet. In response to calls for regulating problematic Internet content, in particular obscene and racial hatred content,[67] the European Commission adopted a Communication on Illegal and Harmful Content (1996b) and a Green Paper on the Protection of Human Dignity in Audio-visual and Information Service (1996a) on 16th October 1996.

A report from the European Commission Working Party (1997) concluded that while the Communication gives policy options for immediate action to deal with harmful and illegal content, the Green Paper aims to promote public debate in order to identify the main problems posed by the new information

[67] The European Commission's resolution of 19th September 1996 voiced its concerns about "the dissemination via the Internet of pornographic and racist material." It called on the Commission to consider "technical and legal measures to combat at European and global level the problem of the use of the information superhighways for criminal purposes, including trafficking in women and children and pornography," and to investigate "measures to restrict access for young people to pornography on the Internet." (European Commission, 1996c, para. 80)

services. Furthermore, the Communication concentrates on the Internet, whereas the Green Paper takes a horizontal approach and a medium-to-long term focus on the issue across all electronic media.

The Communication can be largely divided into four sections. Firstly, it assesses the opportunities which are offered by the Internet. Secondly, it identifies different variations of illegal and harmful content. Thirdly, it describes the technical environment of the Internet. Finally, it gives policy options for immediate action on a technological and legal basis to fight against such content on the Internet (European Commission, 1996b). The Green Paper is composed of three chapters. The first chapter identifies the main problems arising from material in audiovisual information services that are of relevance to the protection of minors and human dignity. It underlines the need not to confuse problems of illegal and harmful content. The second chapter provides an analysis of existing legal and constitutional arrangements at European and national level. The third chapter analyses the situation at the level of the EU with regard to Community law and to co-operation in the field of justice and home affairs (European Commission, 1996a).

Through both documents the European Commission clarified its position on Internet content policy. Firstly, it emphasises that co-operation at an international level is crucial to combating illegal content from different countries. Secondly, it encourages self-regulation of the Internet industry. Thirdly, it supports the use of filtering software and rating systems. The two documents were followed by a report of the European Commission Working Party (1996). The Working Party report underlined responsibilities of both national law enforcement authorities and the Internet industry for restricting illegal content on the Internet, and made proposals for further action. Its proposals incorporated self-regulation of the Internet industry, technical

measures including filtering and rating systems, international co-operation and awareness activities. In particular, the report claimed that the self-regulation system should include "a code of conduct for Internet service providers", "a hot-line for complaint from the public with appropriate safeguards against misuse" and "an independent self-regulatory body, including representatives of industry and users, to advise on whether or not a breach of code of conduct has occurred."

In February 1997 a resolution of the European Council (European Commission, 1997a) approved all these initiatives. In April 1997 the European Parliament (1997) adopted a resolution on the Commission Communication on Illegal and Harmful Content on the Internet. This resolution followed a report of the Committee on Civil Liberties and Internal Affairs (1997). This report underlined the fundamental distinction which has to be made between illegal content and harmful content. It also called on the Commission to propose a common framework for self-regulation at the EU level and to encourage the development of a common international rating system. In July 1997 an European Ministerial conference in Bonn, entitled the Global Information Networks: Realising the Potential, discussed these regulatory approaches. Its Ministerial declaration, *Bonn Declaration*,[68] supported the European Council resolution on illegal and harmful content on the Internet of February 1997 and stated:

> Ministers stress the role which the private sector can play in protecting the interests of consumers and in promoting and respecting ethical standards, through properly-functioning systems of self-regulation in compliance with and supported by the legal system. Ministers

[68] The full text of the *Bonn Declaration* is available on the European Commission Information Society's Archived Website at http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html (Retrieved March 14, 2005)

> encourage industry to implement open, platform-independent content rating systems, and to propose rating services which meet the needs of different users and take account of Europe's cultural and linguistic diversity. (para. 19)

On 27th November 1997 the European Commission (1997b) launched a proposal for an 'Action Plan on Promoting Safe Use of the Internet.' Through the Action Plan, which would cover a three year period from 1998 to 2001, the Commission envisaged four main lines of action: creating a safe environment, including the creation of an European network of hotlines to report illegal content by the public and the development of the Internet industry's self-regulatory schemes for combating illegal content; developing international filtering and rating systems to prevent users from potentially harmful content; encouraging awareness campaigns among the public, in particular parents, teachers and children; and monitoring and support for legal developments in the sector (Akdeniz, 2001b; Pinard, 1998). On 25th January 1999, the European Parliament and the European Council finally adopted the Action Plan, entitled Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (European Commission, 1999a).[69]

Since then, the Action Plan has been one of the major frameworks for dealing with illegal and harmful content on the Internet in Europe. The Action Plan completed its first phase during 1999 to 2001. Its extended second phrase was also completed between 2002 and 2004. As of 2005, the Action Plan is replaced by the Safer Internet *plus* Programme which will take place between

[69] Akdeniz (2001b) explained that the reason for the change of the Action Plan's title from "safe use of the Internet" to "safer use of the Internet" was that "Members of the European Parliament thought that the use of the words 'safer use' would be more appropriate since the EU legislation did not cover criminal law it would not be an easy task to promote 'safe' Internet use."

2005 and 2008.

When compared with other countries discussed above, the European Internet content policy is significant because it emphasises the importance of multi-dimensional regulatory approach to Internet content regulation with a distinction between illegal and harmful content. In particular, it underlines the role of the Internet industry in dealing with illegal and harmful content. However, it does not mean that the EU Internet content policy eliminates the role of the government. It clearly states, "Responsibility for proscecuting and punishing those responsible for illegal content remains with the national law-enforcement authorities." (European Commission Working Party, 1996) For harmonising national laws against illegal content, such as child pornography, the Council of Europe (2001a) introduced the Convention on Cybercrime in 2001.[70] In the same year the EU adopted the Council Framework Decision on combating the sexual expolitation of children and child pornography (European Commission, 2001b).

Although the EU Internet content policy incorporates these advanced features, it has a number of weaknesses. For instance, self-regulation of the Internet industry has been criticised for its lack of public accountability (see Chapter 3.3.2). The technical measures which have been endorsed by the Action Plan, such as filtering and rating systems have been subject to severe criticisms for their inherent technical weaknesses (see Chapter 4 & 5). The issues related to the EU Internet content policy, in particular the Action Plan, will be critically appraised further in Chapter 10.3.

[70] The Convention articulates offences related to child pornography in its Article 9. As of March 2005, the Convention has been signed by 37 member States and 4 non-member States, including Canada, Japan, South Africa and the US.

2.7. A Comparative Analysis of Governmental Internet Content Regulation

These case studies show that each government has a different approach to Internet content regulation. On the one hand, the Chinese government has employed extensive technical measures to control Internet content nationwide and the US government repeatedly introduced legislation which would regulate indecent Internet content with criminal provisions. On the other hand, the EU has adopted a multi-dimensional regulatory approach to Internet content regulation. The UK and Australia's Internet content policies are consistent with the EU policy. However, unlike the UK and the EU, the Australian government has classified Internet content using its national guidelines for films and videos.

First of all, there are different viewpoints on the characteristic of the Internet. As discussed above, while the US Court found the Internet to be a print-like medium, the Australian government recognises and regulates it as a broadcast medium. The question of whether the Internet is a print or broadcast medium is an important issue, because in general each traditional medium has been subject to a different set of regulatory principles and policies. In the UK, print media is free from the government's direct intervention over what can be printed, unless the government obtains a court order for an injunction (Robertson & Nicol, 1992, p. 25). However, radio and television are under the government's legal power. For instance, the Licence Agreement that forms part of the BBC's charter contains clauses which enable the government to control the BBC entirely as follows:

> Section 19 [of the Licence Agreement] enables the Home Secretary, when in his opinion there is an emergency and it is 'expedient' so to act, to send troops in to 'take possession of the BBC in the name and on behalf of Her Majesty.'

> Section 13(4) of the Licence Agreement [...] gives the Home Secretary the right to prohibit the BBC from transmitting any item or programme, at any time (Robertson & Nicol, 1992, p. 26).

Furthermore, Section 10 of *the Broadcasting Act 1990* also gives the government power over commercial broadcasting. It entitles the Home Secretary "to order the Independent Television Commission (ITC) to refrain from broadcasting any matter or classes of matter on commercial television." (Robertson & Nicol, 1992, p. 26) According to Ithiel de Sola Pool, communications law in the US has a trifurcated communication system which consists of three domains of communication; print, common carriers and broadcasting.

> In the domain of print and other means of communication that existed in the formative days of the nation [...] the First Amendment truly governs. [...] In domain of common carriers, which includes the telephone, the telegraph, the postal system, [...] a different set of policies has been applied, designed above all to ensure universal service and fair access by the public to the facilities of the carrier. [...] In the domain of broadcasting, Congress and the courts have established a highly regulated regime, very different from that of print (Pool, 1983, pp. 1-3).

In most modern democratic societies, the print medium is subject to much less regulation, while broadcast is subject to strict governmental regulation on the grounds of a scarcity of usable frequencies in the radio spectrum[71] and intrusion theory,[72] although these regulatory bases have been criticised for

---

[71] see Chapter 2: Footnote 43.

[72] In the case of *FCC v. Pacifica Foundation* in 1978 the US Supreme Court concluded that FCC legitimately has the power to regulate indecent broadcasting. The Court recognised broadcasting as an intruder that is uniquely pervasive not only in public, but also in the privacy of the home, and is uniquely accessible to children [*FCC v. Pacifica Foundation.* 438 U.S. 726 (1978)].

various reasons, such as the advent of cable TV.[73] However, this argument does not mean that the regulatory model of either print media or broadcast media is good enough to regulate the Internet, because the Internet is a complex medium which has characteristics of both print and broadcast media.

Secondly, as regards regulatory solutions, each government discussed above has employed a different mixture of legal and technical regulations on the Internet. Vint Cerf (1994) classified three types of regulation on the Internet: technical constraints, legal constraints and moral constraints. All the governments mentioned have introduced a certain degree of legal constraint to regulate illegal content on the Internet, although there are differences in the extent of the legal constraints. However, their approaches to the technical solutions, such as Internet content filtering systems, are considerably diverse. While the EU endorses the filtering and rating systems primarily to "empower the users to select the content s/he wishes to receive" (European Commission, 1999a), the Chinese government employs various technical measures as a de facto censorship tool. The Australian government also supports the filtering system, but it was introduced under a legal provision.

2.8. Beyond Governmental Internet Content Regulations

In sum, each government discussed above has introduced legal and technical solutions to regulate illegal and harmful Internet content in various ways. Just

[73] Krattenmaker and Powe (1994, p. 204) discuss the concept of scarce resource through their critique of the Red Lion case (see Chapter 2: Footnote 71). They claim, "Scarce resource is a redundant phrase. Every resource is scarce, be it oil, gas, clean water, trees, or iron ore. A nonscarce resource is a contradiction in terms." Also, they deny the intrusiveness of broadcast media. According to them, "radios and televisions are not forced upon citizens, but in fact are considered to be among the most valued household purchases." Robertson and Nicol (1992, p. 594) point out that "the development of fibre-optic cable systems and the advent of direct broadcasting satellites provides viewers with such a multiplicity of choice."

as illegal content in other traditional media has been subject to national laws, so has illegal content on the Internet. In particular, Internet child pornography has been heavily regulated by governments in most countries, including the UK and the US. Indeed, the effectiveness of governmental regulation against the dissemination of illegal content on the Internet cannot be denied. However, the decentralized and transnational features of the Internet have made it difficult to enforce national laws to content. A large amount of Internet content comes from outside a single national jurisdiction and it reflects a different set of socio-cultural standards. This means that individual governments are limited in their ability to exercise regulatory power on content available on the Internet. The difference between the US and European nations' regulatory approaches to racist and xenophobic propaganda is a prime example (see Chapter 2.4.2). Furthermore, excessive governmental regulation on potentially harmful content on the Internet has been subject to strong criticisms. Indeed, "the Internet's architecture does not lend itself easily to hierarchical control." (Liikanen, 2004) Therefore, "a multi-layered approach with the involvement of both public and private regulatory bodies at both national and international level is inevitable to deal effectively" with illegal and harmful content on the Internet (Akdeniz, 2001c, p. 304). In the following chapter, the issues of the multi-layered regulatory approach to Internet content regulation will be discussed in depth.

CHAPTER 3

SELF-REGULATION ON THE INTERNET

3.1. Introduction

As discussed in the previous chapter, the UK and the EU have actively responded to the calls for a multi-layered regulatory approach to Internet content regulation. The 'Action Plan on Promoting Safer Use of the Internet' is a result of this trend. In the course of the development of the EU Internet content policy, self-regulation of the Internet industry has been repeatedly emphasised, alongside creating an European network of Internet hotlines for reporting illegal content by the public and development of filtering and rating systems to prevent users, in particular children, from potentially harmful content (see Chapter 2.6.4.2). In Europe, since the mid-1990s, a number of self-regulatory initiatives have been established, mainly by the Internet industry in support of the EU Action Plan and they have played a key role in the co-regulatory system which deals with illegal and harmful Internet content.

This chapter is not an exhaustive study of all the areas of self-regulation and co-regulation, but it focuses on issues concerning Internet content. The chapter begins with a preliminary discussion about the general definition of self-regulation. This discussion is essential for further understanding of a mechanism of Internet content self-regulation, since the actual status and the initial problems of self-regulation largely depend on its definition as a number of commentators have identified (Price & Verhulst, 2000; Cannataci & Bonnici, 2002).

3.2. The General Definition of Self-Regulation

Self-regulation is not a new concept created by the advent of the Internet era. It has existed and has been sustained in society as one of a number of methods of

regulation of behaviour (Cannataci & Bonnici, 2002).[1] In modern democratic societies, self-regulation structures are broadly adopted by many professional institutions and sectors, ranging from legal and medical professions to financial services, insurance, advertising and the press. A report of the Better Regulation Task Force (1999) defines, "Self-regulation is the means by which members of profession, trade or commercial activity agreed set of rules which govern their relationship with citizen, client or customer."

However, as Gunningham and Rees (1997, p. 364) discuss, self-regulation may take various forms, thus no single definition is entirely satisfactory, because there are many variables of self-regulation, such as the degree of formality, its legal status and the extent of the role played by self-regulatory bodies. Therefore, self-regulation has a range of definitions and it is interpreted in a number of different ways. Indeed, its concept is by no means clear. Monroe Price[2] argues that self-regulation have different meanings depending on who the 'self' is and will differ from nation to nation and sector to sector (Murphy & Blackman, 1999). Irving[3] (1997) argues that at one end of the spectrum, the term self-regulation is used quite narrowly to "refer only to those instances where the government has formally delegated the power to regulate." At the other end of the spectrum, it is used when "the private sector perceives the need to regulate itself for whatever reason and does so."

---

[1] Self-regulation has a long history in European countries, especially in Britain. Since the Middle Ages, under powers granted in royal charters of incorporation, craft guilds discharged supervision of such matters as working conditions, wages, production level and product quality (Ogus, 1992).

[2] Monroe Price is a professor and director at the Cardozo School of Law, Yeshiva University (New York, US). He is also a member of the Advisory Board of the *International Journal of Communications Law and Policy.*

[3] Larry Irving is an assistant secretary and administrator of the National Telecommunications and Information Administration, an agency of the US Department of Commerce.

Baldwin and Cave (1999, pp. 125-126) argue that self-regulation may vary in its different hosts, ranging from individuals to international sectors,[4] thus it may either be voluntary or government controlled to different degrees. At one extreme, for instance, self-regulation may be operated in a purely private sense. In this case, a self-regulatory body may be founded and managed by a private association, which is bound only by its own internal rules. Therefore, there is no interference by governmental institutions and its enforcement powers are extremely restricted. At the other extreme, self-regulation may exist in the context of strong governmental control and public policy tasks are merely delegated to self-regulation agencies by the government. In this case, self-regulation may be approved and operated under governmental supervision.

Depending on the degree of the government's role and influence, self-regulation may be classified into four different types: mandated self-regulation, sanctioned self-regulation, enforced self-regulation and voluntary self-regulation. Julia Black (1996, p. 27) describes the four types of self-regulation as follows:

> [...] *mandated* self-regulation, in which a collective group [...] is required or designated by the government to formulate and enforce norms within a framework defined by the government; [...] *sanctioned* self-regulation, in which the collective group itself formulates the regulation, which is then subjected to government approval; *coerced* self-regulation in which the industry itself formulates and imposes regulation but in response to threats by the government that if it does not the government will impose statutory regulation; and voluntary self-regulation, where there is no active state involvement, direct or indirect, in promoting or mandating self-regulation.

[4] In this sense, a hierarchy of its hosts can be envisaged as one way of conceptualising self-regulation. At the base we have individuals; at the next level we have different market sectors, professional bodies or industrial sectors; at the third level we have nationally organised sectors or bodies and at the peak of the hierarchy we have internationally organised sectors or bodies.

However, apart from the theoretical classification, in practice there is no dichotomy between self-regulation and public regulation. Sinclair (1997, p. 532) argues that an absolute distinction between self-regulation and government regulation cannot be drawn, therefore it may be more accurate and productive to envisage them as being on a regulatory continuum. Indeed, there is a spectrum that contains different degrees of variables as Price and Verhulst (2000, p. 135) point out. In particular, the ideal voluntary model of self-regulation is rare; most self-regulatory bodies are subject to a certain degree of governmental scrutiny.

3.3. Self-Regulation of Internet content: Definition and Aims

What is the definition of Internet content self-regulation? Who is the 'self' in the context of Internet content self-regulation? According to a co-study by Machill, Hart and Kaltenhäuser (2002, pp. 39-40), three distinct groups can be identified in the Internet content self-regulation system: government, users and the Internet industry. They underline the joint development of a code of conduct for the Internet by the Internet industry and users. As regards Internet content, most actively functioned self-regulatory institutions are based on the Internet industry, primarily Internet service providers (ISPs)[5] which "serve as the essential gateways to the Internet and where activity can most closely be observed and supervised." (Jenkins, 2001) In this context, Pierlot (2000) argues that ISPs can, and should, play an important role in empowering Internet users and in dealing with public concerns regarding problematic content.

As the case of the Internet Watch Foundation (see Chapter 3.6.1), some ISPs have taken self-regulatory actions in response to pressure from the authorities.

[5] An encyclopaedic definition of the ISP is "a company that provides Internet services, such as hosting Website, and usually also sells access to the Internet (Pountain, 2003, p. 232).

Edwards (2000, p. 293) argues that:

> [B]ecause ISPs effectively acts as gatekeepers regulating access to Internet content, it is always going to be tempting for state authorities to deem them to be "importers" similar of foreign original illicit material, and therefore responsible for preventing its "entry" or circulation within that state.

The *Somm* case[6] is a prime example of the ISP liability issue. In May 1998, the Munich Administrative Court, German, found Felix Somm, the Chief Executive Officer of CompuServe Europe, guilty of distributing child pornography and other adult content and gave him a two-year suspended sentence (Akdeniz, 2001c, p. 306). In this case, Somm pleaded that CompuServe neither originated this content nor could effectively monitor it. However, the Court claimed that CompuServe had "willfully refrained from deleting child-pornography data for the purpose of making profit" and Somm had "knowledge of such data." (Bender, 1998) Although the decision was reversed by the appeal court in Munich in November 1999, this case has raised the fearful liability issue across the ISP community (Edwards, 2000 p. 293).

In response to ISPs' concern about liability for the Internet content they carry, the European Commission made an effort to address this issue by introducing a proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market in December 1998 (European Commission, 1999c). On 8th June 2000 the European Parliament and Council adopted the proposal as the Directive on electronic commerce (European Commission, 2000).[7] However, the Directive does not provide

---

[6] The full text of the judgment of the *Somm* case is available in English on Cyber-rights.org Website at http://www.cyber-rights.org/isps/somm-dec.htm (Retrieved March 22, 2005).

[7] The Directive came into force on 17th July 2000.

absolute protection for ISPs, but it articulates the conditions of ISPs' liability in its Article 13 and 14. According to Article 14, ISPs are not liable for "the information stored at the request of a recipient of the service," unless ISPs have "actual knowledge of illegal activity or information." If ISPs obtain such knowledge or awareness, they should act immediately to remove or to disable access to the information. In other words, these provisions place an obligation on ISPs to remove illegal content on condition of "actual knowledge." This kind of practice, which is known as 'notice and takedown,' will be discussed later in this chapter (see Chapter 3.3.2 & 3.6.1).

However, Akdeniz (2001b) argues that "the prime responsibility for content lies with authors and primary content providers" rather than with ISPs. He also claims that the government should act against those who create and circulate the content over the Internet and should not force ISPs to resolve the problems related to content (Akdeniz, 2001c, p. 306). Therefore, in my view, the self in the context of Internet content self-regulation should include not only ISPs but also ICPs.

Another issue that needs to be addressed here is the aims of Internet content self-regulation. Before considering such aims, as mentioned in the previous chapter, the distinction between harmful content and illegal content should be clarified. They are very different issues and therefore should be treated with different self-regulatory approaches respectively (see Chapter 2.4.1). As Pierlot (2000) argues, in principle the management and control of harmful content is an issue of user and consumer choice and responsible industry practices, while the control of illegal Internet content is an issue of enforcement. PCMLP[8] (2003) discusses that Internet content self-regulation has several significant aims as follows:

[8] The Programme in Comparative Media Law & Policy at Oxford University.

> Law enforcement. Detection and removal of illegal content through voluntary cooperation of ISPs. This includes: Child Protection (1) preventing profit from and dissemination of child pornography (all countries) and preventing distribution of neo-Nazi, inciting or hate speech (some countries); Child Protection (2) preventing the exposure of children to inappropriate material such as violent or pornographic material; Child Protection (3) preventing dangerous contact / grooming of children.

As the most widespread justification for governmental Internet content regulation has been the protection of minors from illegal and harmful information on the Internet, Internet content self-regulation also has the same object. Indeed, child protection has been the prime regulatory aim not only in the Internet media, but also in other traditional media. In a sense, PCMLP (2003) claims that Internet content self-regulation builds upon a well-established tradition of self-regulation in the media sector from press codes to film rating codes.

3.3.1. Advantages of Internet Content Self-Regulation

What are the advantages of Internet content self-regulation over public regulation? Price and Verhulst (2000, p. 152) argue, Internet self-regulation provides a number of benefits which governmental regulation cannot offer, including efficiency, flexibility, reduced cost and minimised government intrusion in the speech field.

A report of the National Consumer Council, UK (2000, p. 21-22) enunciates a number of the strengths of self-regulation over public regulation. Among them, as regards the content issue, it claims that self-regulation can "more easily deal with matter of subject judgement, such as questions of decency" and "address complex area, in particular where common values and assumptions are shared, without attracting the disadvantages of complex legal requirements."

The first significant advantage of Internet content self-regulation is that it may reduce and reconcile transnational disputes that inevitably occur on the Internet since it has a global architecture. It is often very difficult to apply traditional public law to a case relating to the Internet. The issue of jurisdiction and territorial rights are such examples, since activities on the Internet are not restricted by any territorial borders (see Chapter 2.4). For this reason, Johnson and Post (1996) insist that self-regulating structures are more suitable than any other authorities for solving legal issues on the Internet. Delacourt (1997, p. 208) argues that "the most logical alternative is a consensual regime of user self-regulation" which would avoid the issues of jurisdiction and sovereignty. In practice, in order to overcome transnational issues, different national ISP associations has formed regional ISP associations, such as the EuroISPA.[9] Cannataci and Bonnici (2002) argue that a regional ISP association may be relatively fast and effective at removing illegal content on the Internet, while the states in that region need to take a formal process establishing an intergovernmental legal instrument to achieve the same aims. However, public regulatory authorities have a primary responsibility for fighting against illegal content.

Secondly, from a technical viewpoint, the expertise and technical knowledge of the Internet industry can be more effectively commanded by self-regulatory bodies, while "government agencies may lack the information and technical competence necessary to make the best policy decision." (Price & Verhulst, 2000, p. 150) For instance, no governmental agency can match the accumulated experience and judgment of the Internet sector such as Internet information providers, and ISPs who are able to follow the latest trends on the Internet and to collect a vast amount of information from it, ranging from

[9] The pan-European association of the Internet services providers' associations, EuroISPA, was established on 6th August 1997, in Brussels.

personal and commercial data to confidential information. Therefore, Campbell (1999, pp. 715-716) argues:

> [It] is more efficient for government to rely on the industry's collective expertise than to reproduce it at the agency level. This factor may be particularly important where technical knowledge is needed to develop appropriate rules and determine whether they have been violated.

3.3.2. A Critique of Internet Content Self-Regulation

Self-regulation is not a perfect answer for all, although it may provide more advantages than governmental regulation. Self-regulation has been criticised for three main reasons: a lack of public accountability,[10] ineffectiveness of enforcement and restricting competition.

As regards self-regulation in general, one of the most common critiques is the issue of democracy and accountability of self-regulation. From a legal perspective, Schmitter (1985, pp. 32-62) criticises self-regulation as an example of modern corporatism with the acquisition of power by groups who are not accountable to the body politic through the conventional constitutional channels. Certainly, if a self-regulatory body lacks democratic legitimacy, there is a very strong possibility that the self-regulatory body may misuse its power. In this sense, Ogus (1995, p. 99) argues that if self-regulatory bodies are allowed to formulate and enforce the relevant controls, private interests may gain considerable advantages to the detriment of public interests. Furthermore,

---

[10] According to Ogus (1994, p. 111), there are three different forms of accountability: financial accountability, procedural accountability and substantive accountability. First, in order to ensure *financial accountability*, "regulators should satisfy certain standards of financial management. They should minimise administrative costs and not waste resources." Secondly, "their procedures must be fair and impartial" to fulfill *procedural accountability*. Thirdly, *substantive accountability* is based on the fact that "rules and decisions are themselves justifiable in terms of the public interest goals of the regulatory system in question, whether these be economic or non-economic."

self-regulation may violate procedural accountability, if the self-regulatory bodies cover the whole procedure of regulation, from "policy formulation, interpretation of the rules, adjudication and enforcement as well as rule-making." It is an obvious breach of the separation of power doctrine that is recognised as one of the fundamental principles of democratic societies.

These critiques can equally be applied to Internet content self-regulation. In particular, the ISPs' notice and takedown procedure which is outlined in the Directive on electronic commerce[11] has been criticised for violating due process and rights of appeal. PCMLP (2004, pp. 45-46) points out that ISPs decide legitimacy of Internet content without the proper procedure:

> Whilst [the notice and takedown] system appears to have worked well in the half-decade it has now been running, there does appear to be some danger of confusion about the exact breakdown roles. Hotlines do make a judgement call about whether content is illegal, and ISPs may not [...] invest sufficient time in the review procedure.

Furthermore, PCMLP argues that the 'notice and takedown' is a system that is designed more with ISP liability in mind and less with the objective of preventing illegal or harmful activity. Although it has been argued that self-regulation has the benefit of avoiding state intervention in areas that are sensitive in terms of freedom of speech (Price & Verhulst, 2000, p. 151), in this case, self-regulation could be involved in a private censorship issue (Ahlert, Marsden & Yung, 2004). While the Better Regulation Task Force (1998) identified the five principles of good regulation: transparency, accountability, targeting, consistency and proportionality as a template for testing the appropriateness and effectiveness of regulation, this Internet content self-regulatory practice appears not to provide appropriate transparency and

[11] see para. 46, Article 14(3) and 21(2) of the Directive on electronic commerce (European Commission, 2000. see Chapter 3.3).

accountability.

However, there is a counter-argument that claims that the above criticisms are not necessarily a feature of self-regulation because most self-regulatory bodies are subject to a certain degree of control and scrutiny by government or other independent institutions (Baldwin and Cave, 1999, p. 130). Even if this claim is correct, issues of transparency and accountability still remain crucial to self-regulation of Internet content. In order to make the public trust Internet content self-regulatory mechanisms, Internet content self-regulatory bodies should achieve solid public accountability and effective enforcement. Thus, these self-regulatory bodies must ensure their accountability and social responsibility through monitoring and the enforcement of stringent standards. Furthermore, in order to attain the goals there should be transparency throughout their activities. How can their accountability and transparency be ensured? What can be a practical Internet content self-regulatory model? In the following section, these issues will be discussed in terms of co-regulation.

3.4. Co-Regulation of Internet content

Since self-regulation has been interpreted in a number of different ways, the implementation of content self-regulation on the Internet is also different, sector by sector and nation by nation. As regards the issues of content regulation, the criteria and implementation of Internet content self-regulation can be extremely diverse, depending on the cultural, political, and religious backgrounds of nations or communities. However, many Internet content self-regulatory institutions across Europe and America have adopted a co-regulation model.

A report of the House of Commons' Culture, Media and Sport Committee

(2001, para. 141) defines co-regulation as entailing an "active involvement of Government or regulator." A white paper of the European Commission (2001a, p. 21) states, "Co-regulation combines binding legislative and regulatory action with actions taken by the actors most concerned, drawing on their practical expertise." In this context, as regards Internet content, the concept of co-regulation can be defined as Internet users, the Internet industry and its regulator working together to share responsibility for regulating illegal and harmful Internet content. Machill (2001, p. 34) emphasises that illegal and harmful content should be addressed with a co-regulatory system of responsibility. He claims, "Internet regulation should encompass the duty of all Internet users and commercial providers of services and content to handle data and information only to the extent covered by consent of the parties involved." The National Consumer Council, UK (2000, p. 48) claims that "self-regulation, at its best, can be seen as a co-operation between the regulator, regulated and those in whose interests regulation is made" and recommends that "self-regulation works best within a legal framework."

However, as with the concept of self-regulation, the exact shape of co-regulation can also vary in the way that legal and non-legal bodies are combined and who launches the initiative (European Commission, 2001a, p. 21). In the following section I will examine a European co-regulatory model of Internet content with reference to the EU 'Action Plan on Promoting Safer Use of the Internet.'

3.5. Implementation of Internet Content Co-Regulation: The Safer Internet Action Plan

One of the well-recognised concepts of Internet content co-regulation was outlined by Machill and Watermann in the book, *Protecting Our Children on*

the Internet (2000). It includes five main elements: Internet industry, self-rating and filtering, hotline, law enforcement and media-literacy, for dealing with harmful and illegal content on the Internet (Fig. 3.1).

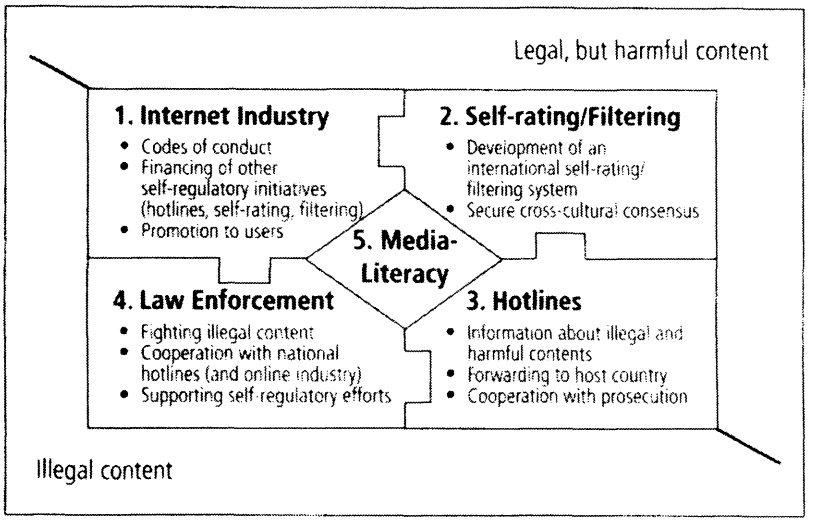

Fig. 3.1. A co-operative regulation model (Waltermann & Machill, 2000, p. 16)

To achieve the effective implementation of this co-operative regulation system, the Bertelsmann Foundation recommended several crucial points at the Internet Content Summit 1999 in Munich (Waltermann & Machill, 2000). First, the Internet industry may develop codes of conduct, in order to ensure that it acts in accordance with its social responsibility. Furthermore, financing self-regulatory institutions that operate hotlines and self-rating/filtering systems would be another important role for the industry. Second, an international Internet content filtering and rating system to secure a cross-cultural consensus would be developed by self-regulatory agencies. Third, hotlines would be established to enable users to report illegal Internet content. Also, it would be preferable for international co-operation between hotlines to be encouraged to effectively prevent illegal Internet content which comes from extraterritorial sources. Fourth, supporting self-regulatory efforts and enforcing legislation to

deal with illegal content and activities on the Internet would be a government's essential role. Finally, as a central element of the system, it is recommended that end-users' computer and media literacy would be strengthened through education and awareness campaigns.

The European Commission has already adopted this co-operative regulation model. In 1999 the Commission launched the 'Action Plan for Promoting Safer Use of the Internet.' As discussed in the previous chapter (see Chapter 2.6.4.2), the Action Plan incorporates four lines of action as follows (European Commission, 2003c, p. 9):

1. Creating a safer environment: creating a European network of hotlines; encouraging self-regulation and codes of conduct.
2. Developing filtering and rating systems: demonstrating the benefits of filtering and rating; facilitating international agreements on rating systems.
3. Encouraging awareness actions: preparing the ground for awareness actions; encouraging implementation of full-scale awareness actions.
4. Support actions: assessing legal implications; coordination with similar international initiatives.

The Action Plan completed its first phase, which covered the period 1999 – 2002, with a budget of 25 million EUR. It involved over 130 different organisations and two service contracts, IAPEXCH[12] and IAPCODE.[13] The Action Plan extended its schedule for two more years, 2003 – 2004, with an additional budget of 13.3 million EUR. (European Commission, 2004a).

[12] IAPEXCH is a contract to provide support to awareness-raising activities. A website, Safer internet.org has been set up to provide information about safer Internet and links to related information (BDRC, 2001, p. 24).

[13] IAPCODE is a contract to provide assistance to self-regulatory bodies in the form of advice. It started work in June 2001 and was conducted by the programme for Comparative Media Law and Policy, Oxford University (BDRC, 2001, p. 24).

During the four year period, a European network of hotlines, INHOPE has been set up (see Chapter 3.6.2). Furthermore, the Internet Content Rating Association (ICRA)[14] has been formed and developed an Internet content rating system. The Action Plan has been a major element in the European Commission's activity against the dissemination of illegal and harmful content on the Internet. The new four-year programme, 'Safer Internet plus', was proposed by the European Commission in March 2004.[15] This Programme is a continuation to the Action Plan. It aims at developing four key areas: fighting illegal content; tackling unwanted and harmful content; promoting a safer environment and raising awareness. It will cover the period 2005 – 2008 with an increased budget of 45 million EUR (European Commission, 2004c).

However, the Action Plan has been subject to a number of criticisms (see Chapter 10.3). In particular, the Internet content filtering and rating system has faced strong critiques. The development of international self-rating and filtering systems has been emphasised by many Internet self-regulatory organisations, such as the IWF, as crucial technical tools for self-regulating Internet content. The ICRA has set itself the task of developing a global Internet content rating system. However, the Center for Democracy and Technology (1999) argues that "promoting a single, comprehensive, global rating system" would jeopardise free speech rights on the Internet. Moreover, many experts argue that self-rating and filtering systems are simply unworkable. Schrader (1999) claims that:

---

[14] The ICRA was formed in 1999, but its origins go back to the foundation of the Recreational Software Advisory Council (RSAC) in 1994. The ICRA owns and operates the ICRA labelling system and its RSACi forerunner (Resource: The ICRA Website. Retrieved March 3, 2001, from http://www.icra.org). In Chapter 5 the ICRA and its Internet content rating system will be discussed in depth.

[15] COM (2004) 91 final. Brussels, March 12, 2004. The Programme is scheduled to be formally adopted by the Council of Europe on 12th April 2005.

> Internet filtering and rating technologies are theoretically unworkable. It is not that they are technologically unworkable, or technologically limited at the present time. [They] are an illusion. They impose a simplistic set of values on a complex and highly variable world of personal tastes, individualised family values, [...] and widely varying thresholds of social tolerance.

The issues relating to filtering and rating systems from both a theoretical and technical point of view will be explored in Chapters 4 and 5.

3.6. Internet Content Self-Regulatory Institutions in Europe

Since the use of the Internet started to explode in the mid-1990s, many Internet self-regulatory institutions have been established in Europe. Self-regulation on the Internet includes a number of issues ranging from e-commerce and technical standards to content control. In particular, self-regulatory bodies have played a decisive role with regard to the technical standards of the Internet, such as the Internet Engineering Task Force (IETF)[16] and the World Wide Web Consortium (W3C).[17] Although the issue concerning these institutions with technical standards on the Internet is a significant field of study, it is beyond the scope of this thesis.

---

[16] The IETF, which was established in 1986, is a self-organised group of people who contribute to the engineering and evolution of Internet technologies. It is responsible for all basic Internet technologies and develops the Internet protocols. An example of Internet self-regulation by the IEFT is the changeover from transfer Internet Protocol version 4 (IPv4) to Internet Protocol version 6.

[17] In October 1994, the W3C was founded by Tim Berners-Lee at the Massachusetts Institute of Technology, Laboratory for Computer Science in collaboration with the European Organisation for Nuclear Research (CERN) with support from the US Defense Advanced Research Projects Agency (DARPA) and the European Commission. The Consortium mainly contributes to efforts to standardise Web technologies by producing specifications, called "Recommendations." The W3C Recommendations include: The HyperText Markup Language (HTML), Cascading Style Sheets (CSS), Extensible Markup Language (XML) 1.0, Platform for Internet Content Selection (PICS) and Resource Description Framework (RDF) (W3C, 2000a).

In the following section, two Internet self-regulatory organisations, the Internet Watch Foundation and INHOPE will be considered. These two organisations have been closely related to the EU Action Plan as discussed above. In particular, INHOPE is a unique organisation which would not have been set up without EU funding. A proposal of the European Commission (2004c) claims that the network of hotlines is a key instrument of the Action Plan and it emphasises that the network should be extended to cover the countries where illegal content is hosted and produced. Therefore, the Internet Watch Foundation and INHOPE will be discussed in the context of the EU Action Plan.

3.6.1. The Internet Watch Foundation, UK

In late September 1996, just three months after the first Internet child pornography hotline was established in the Netherlands, the Internet Watch Foundation (IWF) was launched to address the problem of illegal and harmful content on the UK Internet, with particular reference to child pornography. It was established to implement an industry proposal, 'R3 Safety-Net,'[18] jointly agreed by the government, the police, the Internet Services Providers' Association (ISPA UK), the London Internet exchange (LINX)[19] and the Safety Net Foundation which was subsequently renamed the IWF. Although it is an industry-based independent organisation, the initial impetus of the establishment of the IWF resulted from a potential confrontation between industry and law enforcement. Ruth Dixon, former deputy chief

[18] "R3" referred to the triple approach of the proposal: rating, reporting, and responsibility. The proposal endorsed the establishment of a hotline reporting system and a Platform for Internet Content Selection (PICS) based rating system. It also emphasised the industry's responsible services and self-regulatory efforts.

[19] LINX was founded in 1994. It provides a physical interconnection for its members to exchange Internet traffic through co-operative peering agreements. Currently, it is the largest Internet exchange point in Europe.

executive of the IWF, described the confrontation as follows:

> In August 1996 the Metropolitan Police issued to ISPs a letter naming 133 Usenet newsgroups which were believed to contain illegal pornography. The wording of this letter was perceived as an implicit threat of prosecution for ISPs who failed to drop the groups from their newsfeed, and it was against the backdrop of this confrontational situation that the so-called SafetyNet discussions were held. These brought together industry, government and law enforcement to find a mutually acceptable solution. [This] confrontation became a positive catalyst for [...] practical co-operation between a broad range of different stakeholders (Dixon, 2001).

The three essential roles of the IWF are operating an Internet hotline, promoting voluntary systems for the Internet content rating, the use of filtering software and an education and awareness campaign. These are consistent with the EU Action Plan's three action lines. For promoting the Internet content rating system, the IWF worked on the introduction of the Internet content rating system under the Internet Content Rating for Europe (INCORE) project (Cyber-Rights & Cyber-Liberties (UK), 1997). David Kerr of the IWF submitted the final INCORE report to the European Commission in April 2000 (Kerr, 2000). As regards its hotline function, the *IWF Annual Review 2002* reports that the IWF handled over 17,000 reports through its hotline in the year 2002 — an average of 400 reports a week (IWF, 2003a). However, a report from the Cyber-Rights & Cyber-Liberties (UK),[20] *Who Watch the Watchman*, criticises the IWF for being a subjective private censorship body as follows:

[20] Cyber-Rights & Cyber-Liberties (UK) is a non-profit civil liberties organisation which was founded in 1997. The organisation aims at promoting "free speech and privacy on the Internet" and at raising "public awareness of these important issues." (Resource: Cyber-Rights & Cyber-Liberties (UK). Retrieved June 11, 2004, from http://www.cyber-rights.org/background.htm)

> There are [...] technical problems with the utility of the IWF initiatives where on-line users will report the unwanted materials. Users will probably report material unacceptable according to their taste and moral views, but it should be remembered that it is for the Courts and judges to decide whether something is obscene or illegal. It should also be noted that with reporting systems the interpretation of images will always be subjective. [...] When censorship is implemented by government threat in the background, but run by private parties, legal action is nearly impossible, accountability difficult, and the system is not open and becomes undemocratic. These are sensitive issues and therefore, before introducing these systems there should be an open public debate possibly together with a consultation paper from the DTI. It should be noted that the IWF is predominantly industry based and therefore it does not necessarily represent the public at large and the UK society (Cyber-Rights & Cyber-Liberties (UK), 1997).

Akdeniz (2000, p. 246) also argues that the IWF does not properly cover even the UK ISP industry — just like ISPA UK does not represent the entire industry[21] — thus "the IWF scheme do not necessarily clarify ISP liability at a national level."

Despite these criticisms, the IWF model has been adopted in many European nations, including *Hotline* in Ireland, *Stopline* in Austria, *Safeline* in Greece and *Stop-it* in Italy. In March 1998 the American hotline, *CyberTipLine*, was launched in partnership with the Federal Bureau of Investigation (FBI), Bureau of Customs Immigration Enforcement and the US Postal Inspection Service. As a result, a pan-European organisation, the Internet Hotline Providers in Europe (INHOPE), was launched.

[21] Internet Services Providers Association UK (ISPA UK) was set up to promote self-regulation. The members agree to abide by the ISPA UK Code of Practice which was first adopted in January 1999. As of April 2004 it has 83 members, including AOL Europe, BT and Microsoft, while the total number of ISPs in the UK is 381 according to ISP Review (http://www.ispreview.co.uk, retrieved 16/06/04).

3.6.2. INHOPE

In 1997 a worldwide hotline association was first proposed by Childnet International which is a UK-based non-profit organisation. Under financial backing of the European Commission Daphne programme, [22] Childnet International initiated "a forum for European hotlines to meet and discuss common issues of concern." The INHOPE Association was formally established in November 1999 (INHOPE, 2004a). Since then, it has been partly funded by the EU Action Plan. According to its statement, its mission is "to facilitate and co-ordinate the work of European hotlines in responding to illegal use and content on the Internet." The key functions of the Association are to: exchange expertise, support new hotlines, exchange reports, interface with initiatives outside the EU and educate and inform policy makers, particularly at the international level (INHOPE, 2004b).

By March 2004, INHOPE had 17 full members, two provisional members and one associate member. [23] As discussed, since the Internet has a global architecture, a single nation's Internet content regulatory efforts can hardly be effective. In this sense, international co-operation is essential in enhancing the effectiveness of Internet content regulation. INHOPE is a prime example of International co-operation for preventing illegal information on the Internet. According to a white paper produced by INHOPE, *A Safer Internet for All*, "the broad network coverage, the exchange of reports about illegal content, the

[22] The DAPHNE Programme is a community action programme to fight violence against women and children. It was set up by the European Commission. Five million EUR was spent each year under the Programme from 2000 to 2003.

[23] The members of INHOPE include various organisations ranging from government agencies, such as ABA (Australia) and ICEC (South Korea), and industry-based organisations, such as IWF (UK) to independent charity organisations, such as Save the Children. Although each member has a different background, all the members are working in close co-operation with Internet industries, polices and governments (Resource: INHOPE Website. Retrieved March 14, 2004, from http://www.inhope.org/english/about/members.htm).

varied background and expertise of its membership organisations, the sharing of expertise and knowledge and the respect for culture and legal diversity across the membership base has demonstrated the effectiveness of the hotline network." (INHOPE, 2003, p. 14) The so-called Operation Hamlet is an example of how INHOPE works in supporting law enforcement activities.

> During 2002 a member of the public made a report to the Swedish Hotline. When the report was processed, the hotline staff recognised a logo on a tea-shirt worn by the perpetrator and identified likely country as Denmark. The report was forwarded to the Danish Hotline and Danish Police for further investigation. As a result of a swift investigation, the paedophile was arrested and victim rescued and taken into care. A joint investigation by the US Customs Service and the Danish National Police targeted the ring of paedophiles, which this perpetrator was a member, who molested their own children and distributed the images on the Internet. As a result of this operation up to March 2003, there have been 16 US Search Warrants issued, 19 US Arrests, 12 International Arrests, and over 100+ children rescued (INHOPE, 2003, p. 12).

Indeed, INHOPE has achieved widespread and effective co-operation. It has successfully expanded membership not only within Europe but also at an international level. As of March 2004, it has members in four non-European nations: Australia, South Korea, Taiwan and the US (see Chapter 3: Footnote 23). The European Commission (2003c, p.4) argues that the role of INHOPE is extremely important in the implementation of the EU Action Plan. Furthermore, the latest 'Safer Internet plus' programme strongly supports INHOPE under its first action line, 'Fighting against illegal content.' (European Commission, 2004c)

Although hotlines have been adopted as a key instrument for preventing illegal Internet content, it is essential to ensure that the primary responsibility for

fighting against illegal content rests with law enforcement authorities. INHOPE has clearly defined its position in its report (INHOPE, 2002, p. 4):

> Hotlines must provide a mechanism for receiving complaints from the public about alleged illegal content and/or use of the Internet; they must have effective transparent procedures for dealing with complaints and they must have the support of government, industry, law enforcement, and Internet users in the countries of operation.

The European Commission (2004c, p. 7) also states that public authorities, such as the police, public prosecutors and the courts, are in the forefront of the fight against illegal content. Only they can ensure that offenders are brought to justice. Internet hotlines are secondary in the context of illegal Internet content regulation.

However, INHOPE is also subject to the criticisms which the IWF comes under. Nadine Strossen, ACLU president, criticised "a plan to establish [...] hotlines that the public can use to report objectionable Internet content, saying that it turns hotline operators into 'self-appointed judges of law' and encourages vigilantism." (ACLU, 1999c)

3.7. Conclusion

The first significant feature of Internet content regulation in Europe is its multi-layered regulatory approach which incorporates hotlines, filtering/rating systems and awareness campaigns. Furthermore, it draws a distinction between illegal content and harmful content and takes a separate regulatory approach to each issue. While it endorses a network of Internet hotlines for reporting illegal content by the public, it supports the development of filtering and rating systems for preventing children from accessing potentially harmful Internet content.

The second significant feature is that it underlines co-operation; from domestic co-operation between various parties who are involved in the self-regulation system, including government, industry, and civil organisations to international co-operation between nations. The European Commission (2004c) states that international co-operation will be an integral part of the action of its new 'Safer Internet plus' programme.

Although the co-operative regulation model, which is based on self-regulation, has become a mainstream of Internet content regulation in many European nations, its practical effects are still debatable. As mentioned above the industry-based hotlines have been criticised for privatised censorship. In particular, technical solution-based regulation, such as filtering and rating, has raised various controversial issues concerning not only free speech rights but also their technical effectiveness. Moreover, in my view this model may not be acceptable or may be impractical in some other countries. In this model, co-operation would be based on a mutual understanding and well-balanced power between each party. In some countries, where the government monopolises all the power of Internet regulation and where the industry has no accumulated experience of self-regulation, this model cannot work properly. I will discuss this issue through a case study of the Internet content regulation in South Korea in Chapter 9.

CHAPTER 4

THE FIRST GENERATION FILTERS

4.1. Introduction

As the Internet has allowed information to be circulated with the speed of light and regardless of frontiers, contents which are deemed to be illegal and harmful have also been disseminated. Since the use of the Internet has proliferated, the availability of such content has been a great concern to both governments and Internet users. "A May 1999 survey of US parents showed that 78% have concerns about the content of Internet material to which their children have access." (Cabinet Office, 1999, para. 10.13) As discussed in the previous chapters, illegal content and harmful content are significantly different issues. Each issue requires a separate regulatory solution. While in principle the control of illegal Internet content is an issue of enforcement, the management and control of harmful content is an issue of user and consumer choice (Pierlot, 2000). In this context, Internet content filtering technologies have been developed for enabling users to deal with harmful content.

In recent years, commercial filtering software has become massively popular. Many proponents, including parents, teachers and governments, have chosen commercial filtering software as a feasible technical solution for protecting minors from harmful information on the Internet, such as child pornography and obscene material. They argue that filtering software has enhanced affectivity and reliability for years, as proven by their popularity in the marketplace. Indeed, during the last few years, with the exponential rise in popularity of the Internet, the Internet content filtering software market has grown significantly. The US market is a prime example. According to a research firm, Frost & Sullivan, in 2000 the revenues of content filtering in the US market alone reached 119 million USD and this is expected to have grown to more than 1 billion USD by 2007 (Bannan, 2001).

4.2. Technical Aspects of First Generation Filtering Software

4.2.1. Definition

On the Internet filtering is a technical mechanism for sorting content into categories for the purpose of decreasing accessibility of certain type of content. In general, filtering software is designed in order to prevent Internet access by monitoring user requests and by interceding between user and connection to the Internet. Jonathan D Wallace[1] defines filtering software as follows:

> Software products published by commercial software publishers which do any of the following: block access to Internet sites listed in an internal database of the product; block access to Internet sites listed in a database maintained external to the product itself; block access to Internet sites which carry certain ratings assigned to those sites by a third party, or which are unrated under such a system; scan the contents of Internet sites which a user seeks to view and block access based on the occurrence of certain words or phrases on those sites (Wallace, 1997a).

Currently, there are several different filtering technologies on the Internet: keyword screening, blacklist filtering, whitelist filtering, packet filtering, image analysis filtering, label filtering and so on. Amongst them filtering based on database and keyword or phrase are usually referred to as first generation filtering – rating and labelling systems will be explored in depth in the next chapter. These first generation filtering systems have been the dominant filtering methods of commercial Internet content filtering products, while the European Commission has preferred label filtering systems that are based on

[1] Jonathan D. Wallace publishes an online magazine, *Ethical Spectacle* (http://www.spectacle.org/) and is co-author of *Sex, Laws and Cyberspace* (1996). He was a co-plaintiff in *ACLU vs. Reno*, which challenged the CDA.

the Platform for Internet Content Selection (PICS) (see Chapter 5.2.1) as opposed to first generation filtering software as a technical solution for preventing illegal and harmful content on the Internet. The first generation filtering technologies are still used alone or in combination by most commercial filtering software in the current marketplace. Although first generation filtering technologies have a number of technical limitations, they are apparently considered to be a feasible tool for addressing issues of inappropriate content on the Internet. In this chapter first generation filtering will be explored and its advantages and drawbacks relating to end-users' autonomy and freedom of expression will be discussed.

4.2.2. Methods of Filtering

First generation filtering technologies can be divided into two major types that are used as the basis for most commercial filtering software; Uniform Resource Locator (URL) filtering and keyword-based filtering.

URL filtering which blocks a site based on its URLs is the most common form of filtering. This is divided again into two different types; blacklist and whitelist filtering. Blacklist filtering employs a blacklist of unwanted URLs. Such a list is normally classified into a variety of categories, for instance crime, drugs, religion, sex, and violence. A categorisation list is formed by a filtering software vendor in roughly three steps as follows:

> 1) developing a list of websites for possible categorisation; 2) using automated systems [such as Web crawlers[2] and other Artificial Intelligence-based information extraction programmes] to examine

[2] A crawler is a programme that visits Websites and reads their pages and other information in order to create entries for a search engine index. It is also known as a spider or a bot.

> each page or site and to recommend possible inclusion in one or more blocking categories; and 3) in many (but not all) instances, using human reviewers to make the ultimate decision about whether and how to categorise each page or site (Edelman, 2001).

Whitelist filtering is an alternative approach to blacklist filtering. Users are permitted to access only URLs that are included in the whitelist. Consequently, access to material is heavily limited. It is intended mainly for pupils or closed communities.

Keyword-based filtering is another common form of filtering. It uses text search to categorise sites. If a site contains any word or phrase, for instance porn, sex, or breast, on a blacklist that is given either by filtering software producer as a default option or by end-user, it will be blocked. It cannot be used to block visual information.

There are other filtering methods such as packet[3] filtering and images analysis filtering. However these filtering methods are not widely used as the basis of filtering software, because of their serious technical shortcomings.

Packet filtering operates by examining IP addresses on a router.[4] The Internet information is delivered in the form of a packet which has a peculiar Internet Protocol (IP) address. Thus, certain Internet content can be blocked through filtering a specific IP address. However, since an IP address does not represent a Website, but a particular computer, blocking an IP address may block many other lawful Websites that happen to be hosted on the same computer. Since this technical drawback is inherent, no commercial filtering software currently

---

[3] see Chapter 1: Footnote 2.

[4] A router is "a hardware device that connects two or more networks or network segments together to form a single internetwork, by forwarding data packets from one network into another." (Pountain, 2003, p. 380)

employs the packet filtering method.

Images analysis filtering is a relatively recent approach. Since discussing in detail mechanism of image analysis technology is beyond the focus of this thesis, discussion of it here will be brief. Images analysis technology is currently utilised only in a few fields, such as character, fingerprint, and visage where a sum of available images' number is limited, while the variety of images which are available on the Internet is virtually unlimited. Furthermore, this technology is not designed for a value judgment, in that it never distinguishes between masterpieces and pornography. Of the ten leading examples of commercial filtering software reviewed in the section below, no software uses image analysis filtering.

4.2.3. Locations of Filtering

Internet content filtering can be used not only by an end-user, but also by an Internet Service Provider or a third party.

An end–user can block certain information using stand–alone filtering software on the user's own personal computer. The software checks the user's request against a given blacklist or whitelist or keyword list. The request is then either allowed or blocked (Fig. 4.1).

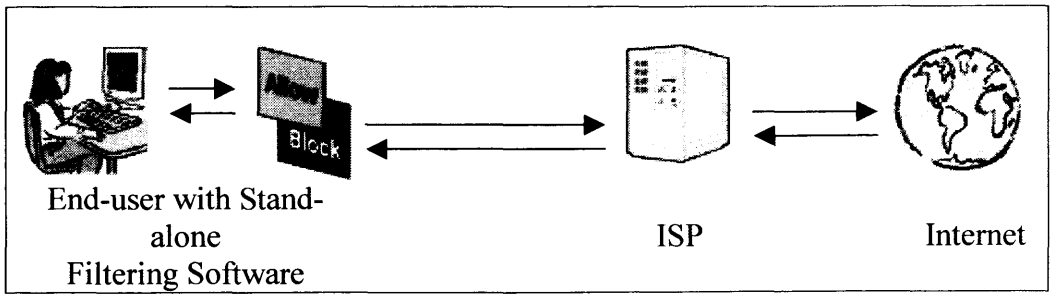

Fig. 4.1. Filtering at an end-user level

Moreover, an end-user's request can be checked by the ISP (Fig. 4.2).[5]

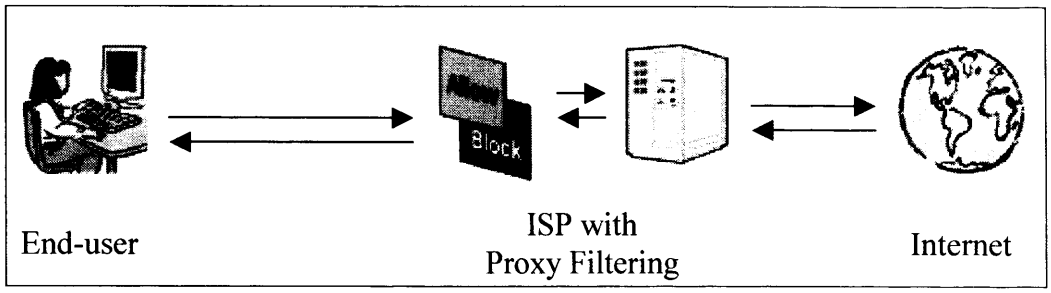

Fig. 4.2. Filtering at a ISP level

However, filtering by ISPs employs several techniques which are different from end-users' filtering. Among ISPs filtering techniques proxy filtering is the most common form, because no client of the ISP can bypass the proxy server to access the Internet legitimately. A report from the Commonwealth Scientific & Industrial Research Organisation (CSIRO, Australia) describes the process of proxy filtering as follows:

> When a user requests a particular Web page or ftp file, the following takes place: The proxy server checks to see if the requested URL is on its filter list; If the URL is on the filter list, the user is informed accordingly that the page or file is unavailable; If the URL is not on the filter list, but is currently in the cache of the proxy server (as a result of having been requested recently by another user), the requested page or file is sent to the user from the proxy; If the requested material is not in the proxy server cache, the ISP issues a request for the material from its source on the Internet (Greenfield, McCrea & Ran, 1999).

A third party which is appointed by the ISP can check end-user's requests that

[5] In the UK AOL (http://www.aol.co.uk) provides a server-based filtering software, AOL Parental Controls, as a part of the AOL service. In addition, several US-based ISPs have offered a pre-filtered Internet access, such as Cybersouth Networks (http://www.cybersouth.com), Dnet (http://www.dnet.net) and Safe Access (http://www.safeaccess.com). All these Websites were visited on 10th December 2001.

are directly passed through the ISP. To fulfil this third party filtering, the end-user's Web browser must be set to point to the third party's Website (Fig. 4.3).

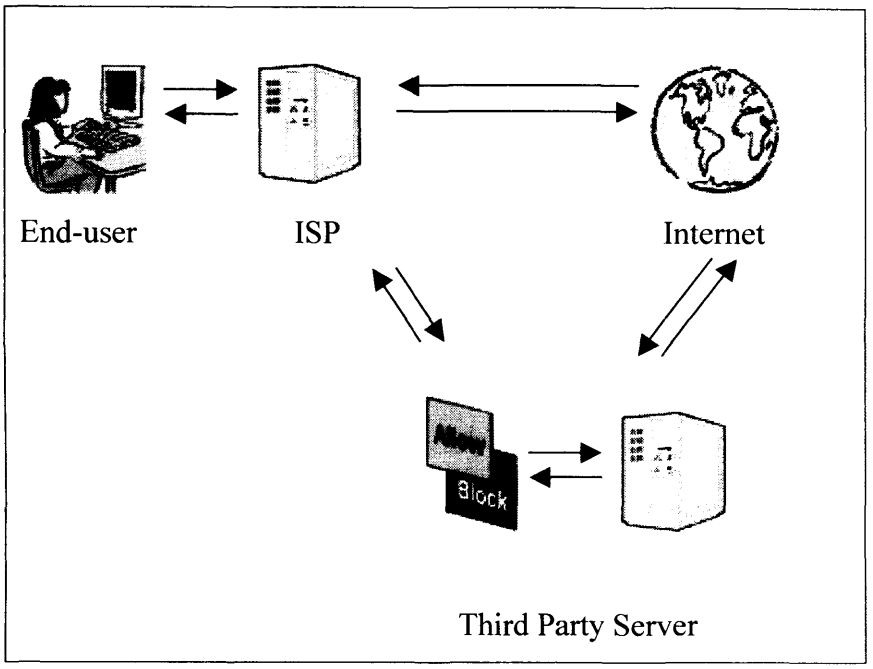

Fig. 4.3. Third-party filtering

4.3. Technical Review: 10 Examples of Commercial Filtering Software

In order to examine how the filtering technologies are applied to commercial products in practice, I shall now review ten stand-alone filtering software products which are designed mainly for home-users. I evaluated each product using the following six criteria; filtering coverage, filtering methods, reporting, customisability, usability, and effectiveness which are the main features that indicate the performance of filtering software. In addition, each product's technical specifications were compared with the others (see Appendix A and B). All products were purchased over the Internet. They were downloadable from their own Website and seven products offered free trial versions. One product was a freeware. Unfortunately, only three products were available as a package

at UK-based online-shops. The software are listed in alphabetical order: Cyber Patrol 5.0, Cyber Sentinel 2.0, CYBERsitter 2001, Cyber Snoop 4.0, Net Nanny, Norton Internet Security 2002, N2H2, Pure Sight 2.5, We-Blocker 2.01, X-Stop. Each product's price, subscription fee, and free trial version are as follows. This review was conducted in December 2001 (Table 4.1).[6]

	CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Price (GBP / *USD)	39.95	46.94	39.95*	49.95*	34.99	41.86	39.95*	39.95*	Free	60.00*
Subscription (GBP / *USD)	39.95	—	Free	—	16.95*	Free	—	—	Free	Free
Downloadable	•	•	•	•	•	•	•	•	•	•
Free trial available	•	•	•	•	✘	✘	•	•	Free	•
UK-based online shop	✘	•	✘	✘	•	•	✘	✘	✘	✘

Table 4.1. Filtering products

Note: •=Yes ✘=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

[6] In April 2005 a brief review on these software products was conducted in order to check their updated features. As of April 2005, Cyber Snoop and We-Blocker have not been upgraded since December 2001. N2H2's home user version is not available any more. N2H2 works only on a sever computer.

4.3.1. Filtering Coverage[7]

	CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Websites	●	●	●	●	●	●	●	●	●	●
FTP sites	✘	●	●	●	✘	✘	✘	●	✘	●
E-mail	✘	●	●	●	✘	✘	✘	✘	✘	✘
Newsgroups	●	●	●	●	●	✘	✘	✘	✘	●
Chat	●	●	●	●	●	✘	✘	✘	✘	✘
Applications	●	●	✘	✘	✘	●	✘	✘	✘	✘

Table 4.2. Filtering coverage

Note: ●=Yes ✘=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

Although the World Wide Web is the dominant form of the Internet, the Internet provides many different types of communication methods, ranging from e-mail and newsgroups to Internet Relay Chat.[8] Each method uses a diverse protocol; for instance, the Post Office Protocol 3 (POP3) and Simple Mail Transfer Protocol (SMTP) are used for receiving and sending e-mail, and newsgroups use the Network News Transfer Protocol (NNTP). The File Transfer Protocol (FTP) is also one of the Internet protocols.

Thus, unwanted information can be found via FTP sites, e-mails and newsgroups as well as via Websites. According to reports from the Internet

[7] Since December 2001, there has not been a significant change in their filtering coverage. As of April 2005, Cyber Sitter extends its filtering coverage to File Sharing Protocol. Notably, five products, Cyber Patrol, Cyber Sentinel, Net Nanny, Norton Internet Security and X-Stop (renamed 8e6Home) filter online and offline applications, ranging from peer-to-peer software and instant messengers to word processing products.

[8] Internet Relay Chat (IRC) is a system for chatting that involves a set of rules and conventions and client/server software.

Watch Foundation (IWF) during the six years, from 1997 to 2002, *the Internet Watch Foundation Annual Report* and *the Internet Watch Foundation Annual Review*, the Usenet which is known as a newsgroup has been a significantly problematic part of the entire Internet. The report states that until the year 1998 the vast majority of actionable items, which the IWF has judged to contain potentially illegal material, consisted of Usenet news articles with 73 percent, followed by Websites with 22 percent (IWF, 1999).[9] Since that time, simultaneously with the explosive development of the World Wide Web, the proportion of Usenet articles among the IWF's actioned items has significantly fallen to five percent by the year 2002 (IWF, 2003a). However, *the Internet Watch Foundation Annual Review 2001* states, "the role of newsgroups in spreading child pornography round the world [still] continues to attract great concern." (IWF, 2002)

In this sense, filtering software should be capable of filtering not only Websites but also other Internet communications. However, disappointingly, some of the software reviewed for this study filters only Websites. While all ten products work on Websites, only three products cover Websites, FTP sites, e-mail and newsgroups altogether. Cyber Sentinel, CYBERsitter and Cyber Snoop, cover all five Internet communication areas. However, Cyber Sentinel's performance

[9] According to the statistics from IWF, its "Actioned items by Internet location" (1997-2002) is as follows:

Year	Chatroom	E-mail	Usenet	Proprietary Groups*	Web	FTP	Offline	Police Intelligence
1997	4	19	118	0	95	1	2	0
1998	11	11	325	0	104	0	3	0
1999	9	22	498	0	680	0	7	0
2000	8	13	252	0	2094	0	7	4
2001	3	1	317	164	2444	0	1	78
2002	11	2	216	228	3317	3	3	274

* A facility offered by some ISPs to enable groups of like minded individuals to share information in a collective environment.

is unsatisfactory because it simply blocks or allows entire e-mail protocols, FTP sites or newsgroups. N2H2 and We-Blocker filters only Websites.

Notably, three products, Cyber Patrol, Cyber Sentinel, and Norton Internet Security filter even offline applications. For instance, I found that when I opened a Microsoft Word file of this chapter Cyber Sentinel blocked it because of some words in this chapter such as 'pornography.' Moreover, Cyber Patrol can restrict any application by time and access settings. Using Norton Internet Security, parents or administrators can choose categories[10] of Internet-based applications such as Web browsers and e-mail programmes which parents or administrators want to permit their children or other end-users to access.

4.3.2. Filtering Methods

	CP[11]	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Blacklist	●	●	●	●	●	●	●	●	●	●
Whitelist	●	●	●	●	●	●	●	●	●	✘
Keyword	●	●	●	●	●	✘	●	●	●	●
Time control	●	●	●	●	●	✘	✘	✘	✘	✘
PICS-compliant	●	✘	●	●	●	✘	✘	●	✘	✘

Table 4.3. Filtering methods

Note: ●=Yes ✘=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

[10] Norton Internet Security maintains a list of categorised applications that covers hundreds of Internet-based programs. Its twelve categories are as follows: General, Chat, Conferencing & Collaboration, E-mail, Education & Family, File Transfer, Instant Messaging, Newsreaders, Networked Games, Web Browsers, User Categories 1, and User Categories 2.

[11] The latest version of Cyber Patrol (7.0) does not support a PICS-based rating system.

As mentioned above, there are two very common first generation filtering methods; URL filtering (blacklist and whitelist filtering) and keyword-based filtering. Here, these two methods are used alone or in combination as the basis of ten kinds of filtering software reviewed. All ten products employ blacklist as the basis for filtering software. Apart for X-Stop, nine out of ten also use whitelist filtering. Keyword-based filtering is used by nine, excluding Norton Internet Security. All eight products which employ these three filtering methods allow users to use them at the same time (Table 4.3). However, when a user uses them together in practice, whitelist overrides other filtering methods, because whitelist filtering permits users to access only URLs that are included in the whitelist.

Alongside the typical filtering methods, time filtering is employed by five out of ten; Cyber Patrol, Cyber Sentinel, CYBERsitter, Cyber Snoop and Net Nanny. By using time filtering parents or administrators can restrict children's or other end-users' Internet access based on a customised time setting. They can set a time schedule for Internet access, such as daily and weekly limits on the amount of Internet use and specific times each day when access is allowed or blocked (see Fig. 4.4). For instance, parents may allow their children's Internet surfing only on weekday evenings and at the weekend when they may be available for supervising their children's activities on the Internet. In my view this is a powerful alternative to typical filtering methods. While other filtering methods have been criticised for their inherent technical limitations, such as over-blocking and under-blocking, time filtering can avoid this kind of criticism.

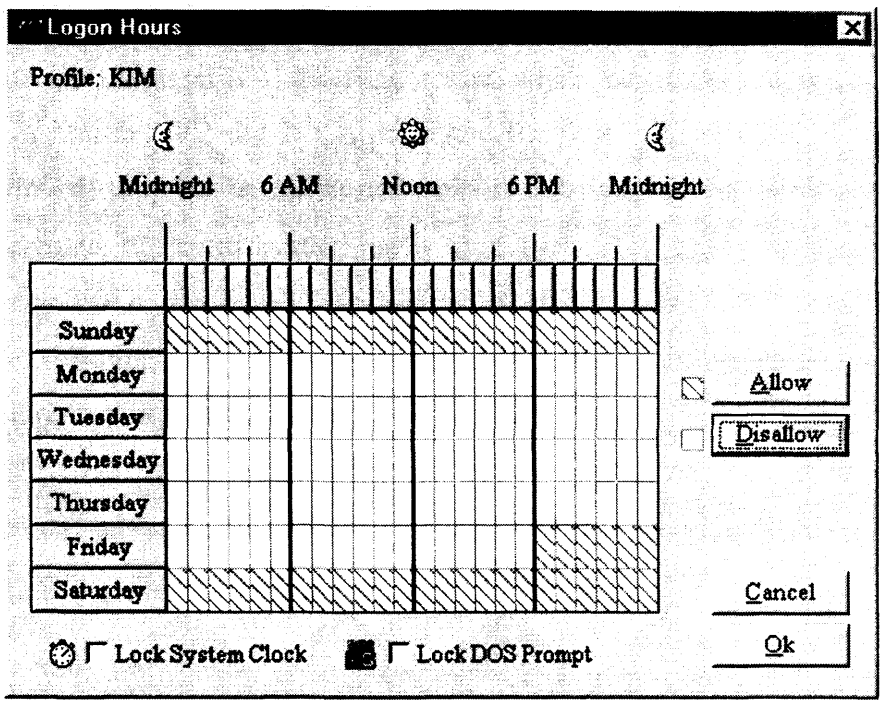

Fig. 4.4. Cyber Snoop's 'Time Controls.' The above setting means that Cyber Snoop allows a user, who is named KIM, to have access the Internet from Friday after 6pm until Sunday 12pm. It also provides a function to lock a user's system clock, in order to prevent her or him circumventing this time control.

Furthermore, five products support PICS-based rating system, such as RSACi (Recreational Software Advisory Council on the Internet, see Chapter 5.3.2)[12] and SafeSurf.[13] It is notable as an example of how first generation filtering software can be combined with rating systems. However, no software yet

[12] In 1994 US Senators Lieberman and Kohl introduced legislation to create a government-run ratings board for computer and video games, but gave the industry one year to create a self-regulatory scheme. In the same year, The Software Publishers Association and five other US trade associations met to create the Recreational Software Advisory Council and to develop the first ever content rating system. On 8th September 1994 RSAC incorporated as a non-profit organisation in Washington. In July 1995 Stephen Balkam, the first RSAC Executive Director, testified to the Senate Judiciary Hearings on Pornography and the Internet and committed RSAC to develop a self-rating content rating system for the Internet. A few months later, in November 1995, RSACi (RSAC on the Internet) Working Group had its first meeting with representatives from Microsoft, ATT, Bell Atlantic, Time Warner, W3C and others. Finally, RSAC announced its rating system in February 1996.

[13] The SafeSurf Internet Rating Standard was developed by Ray Soular and Wendy Simpson in 1995.

provides the latest global PICS-based rating system, the Internet Content Rating Association (ICRA) labelling system which was launched in December 2000. In March 2002 the ICRA published the first version of its own filter, *ICRAfilter*. It supports blacklists and whitelists. As well as the user's own lists, those created by 'third parties' such as a variety of organisations, special interest groups and commercial concerns are also supported (ICRA, 2002). In the next chapter, this ICRA's filtering software will be explored in depth alongside the ICRA rating system.

In addition, uniquely, Pure Sight employs Artificial Intelligent (AI) filtering. PureSight Inc., the producer of Pure Sight claims that:

> The PureSight dynamic filter is based on sophisticated propriety Artificial Content Recognition (ACR) technology, that can "identify" the content of a site and then decide whether to allow its compliance with corporate, institutional, or parental usage policies. PureSight provides complete and reliable Web coverage with unmatched recognition accuracy. ACR is the core technology in the engine that power PureSight. It comprises a power set of Atrificial Intelligence algorithms that analyse and categorise data in real-time (PureSight Inc., 2004, p. 12).

However, I doubt this self-promotion. Although the worldwide computer industry has spent an enormous amount of money on developing AI over the past three decades, even world-class researchers have yet to come up with an AI which is able to recreate human intelligence. In the 1980s, AI research focused on creating machines that could solve problems and reason like humans. Since the early 1990s, however, research has been concentrated on developing smaller, independent robots instead of trying to mimic human intelligence. This is "insect intelligence, which is – in its own way – very sophisticated." Nowadays, AI is all around us. "It is present in computer games,

in the cruise control in our cars and the servers that route our e-mail." (BBC, 2003) Nevertheless, no AI is able to carry on a seamless conversation with a human (Turkle, 1997). It faces serious difficulties in dealing with contextual value. For instance, it simply cannot "understand why it is a bad idea to spread toothpaste on toast." (Kahn, 2002) In this sense, it is unlikely that a small filtering software company is able to develop an AI filter which truly understands the context of human language. This is why other filtering software, such as N2H2 and X-Stop, claim that they employ a combination of Artificial Intelligence technologies and human review.[14]

4.3.3. Reporting

	CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Report	●	●	●	●	●	●	✘	●	●	✘
E-mail report	✘	●	●	✘	✘	✘	✘	✘	✘	✘
Local warning	●	●	✘	●	●	●	●	●	●	●

Table 4.4. Reporting

Note: ●=Yes ✘=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

Reporting is another main feature of filtering software. Usually, filtering software monitors a user's Internet activity, then saves it as a log file for parents' or administrators' viewing. Apart from N2H2 and X-stop, all products provide a reporting function. In particular, Cyber Sentinel and CYBERsitter send parents or administrators a report via e-mail. A user can configure Cyber

[14] According to the 8e6 Technologies, X-Stop uses a Web crawler, the Mudcrawler, which is an array of highly advanced search devices designed to identify pornographic sites for blocking. The Mudcrawler seeks out pornographic and obscene material and after human verification, the sites are categorised in the X-Stop library.

Sentinel to send her or him an e-mail when a violation occurs or after a certain amount of violations are logged. CYBERsitter can send a user daily reports containing the previous day log file and system status by e-mail. This kind of automatic reporting function makes it possible for parents easily and efficiently to keep track of their children's activities on the Internet, even if parents are in their workplaces.

On this criterion Cyber Snoop's performance is impressive. Cyber Snoop displays a copy of monitored Internet activity and allows parents or administrators to link back to actual Websites visited. It also restores the text of incoming and outgoing news, e-mail, chat and Instant Messenger items, allowing parents or administrators to maintain a history of all Internet activity for review. Its 'Top Ten Reports' provide data on Internet activity, such as top ten transactions, top ten Websites visited, top ten e-mail addresses, top ten Internet users and so on. A user can also control the size of the current activity log by archiving old data. Cyber Snoop automatically performs an archive of the current activity log and its associated cache files. Then, the archived data is stored in the local or network directory specified by the user.

4.3.4. Customisability

All software reviewed for this study provides some degree of customisability. In particular, all filter lists can be customised or modified according to user preference. Users can choose certain categories of filter lists. For instance, a user can configure Cyber Patrol to filter only sites which are categorised as 'Full Nudity' and 'Sexual Acts', while a user can access other sites which are under the rest of categories such as 'Sex Education' without filtering. Furthermore, a user can manually add or delete a site or word from filter lists.

Although the filter lists can be edited, they are not viewable to users in eight out of ten of the software I reviewed. Only two products, Cyber Snoop and Net Nanny, provide transparent filter lists. These two products' block list windows are shown as follows (Fig. 4.5 and 4.6). Cyber Snoop's filter list includes 14,719 websites, from http://100amateurs.com/ to http://youngluv.sexpussy.nu/, in alphabetical order. Most Websites on their block lists are Websites which provide pornographic or sex-related information:

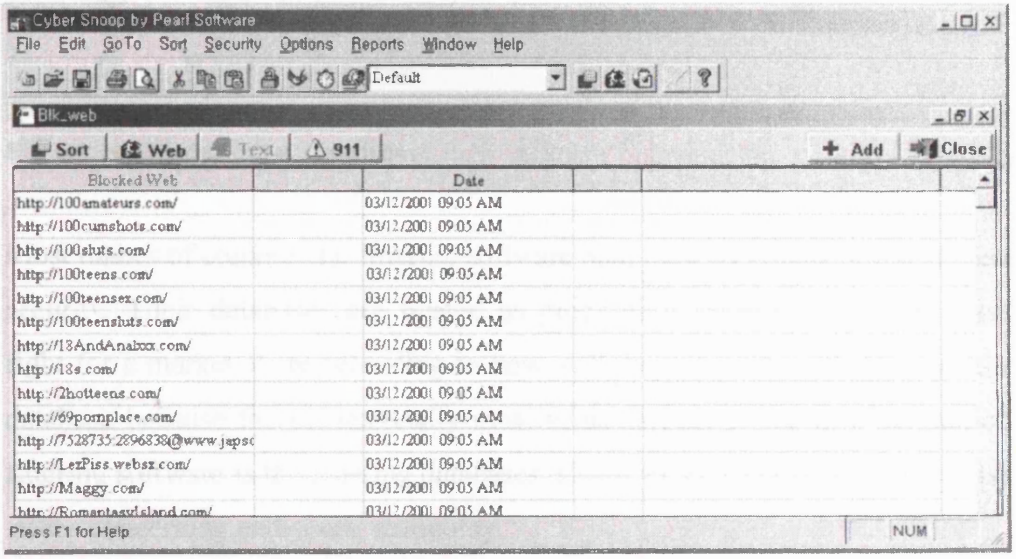

Fig. 4.5. Cyber Snoop's block list window.

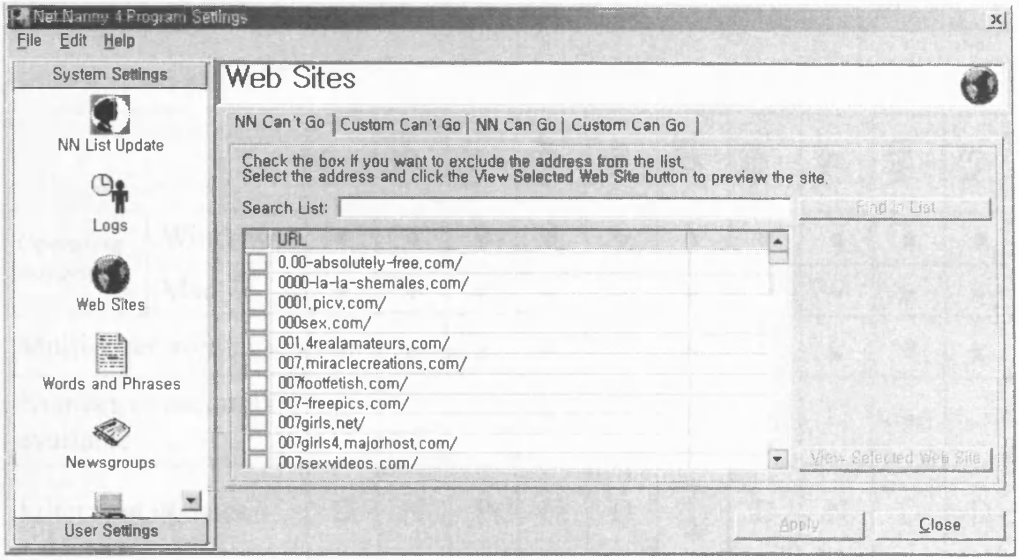

Fig. 4.6. Net Nanny's block list window.

Most makes of commercial filtering software hold their filter lists in the highest security. Their databases are treated as proprietary information. Companies fight for a market share according to how well they upgrade and maintain the database because the commercially most valuable part of the first generation filtering software is the filtering databases. However, encrypted filter lists raise issues concerning end-users' autonomy.

In addition, all ten software products allow a user to select any combination of filtering methods. A user can turn off a keyword filtering option while she or he uses a URL filtering or PICS-based rating option.

4.3.5. Usability

		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Operating System	Windows	●	●	●	●	●	●	●	●	●	●
	Mac	●	✓	✓	✓	✓	✓	✓	✓	✓	✓
Multi-User accounts		●	✗	✗	●	●	●	●	✗	●	✗
Number of accounts available		(9)	—	—	(UL)	(12)	(UL)	(UN)	—	(UN)	—
Filter List updates		D	N	P	N	D	2 W	D	N	D	D
Number of categories		12	(UN)	30	(UN)	5	31	40	2	7	34

Table 4.5. Usability

Note: ●=Yes ✗=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop **D**=Daily, **P**=Periodical, **2W**=Every two weeks, **N**=None, **UL**=Unlimited, **UN**=Unknown

Installation and setup

Overall, installation and setup is fairly easy and simple. Although Cyber Patrol and X-stop constantly crash using Microsoft Windows 2000, they are working well with Microsoft Windows 98 second edition. Filtering products are usually small in size. Of the ten that I reviewed, six software packages require no more than 20 megabytes hard disk space. CYBERsitter and N2H2 need only two and three megabytes hard disk space respectively. All ten products also require no more than 32 megabytes RAM (Random Access Memory).

Platform

Unfortunately, Mac Users have few choices when they want to use filtering software, while all the ten products are compatible with the Microsoft Windows operating systems, including Windows XP. Among the ten products,

Cyber Patrol was the only product which provides a Macintosh version. However, the latest version of Cyber Patrol (version 6.0) is not compatible with the Macintosh operating system. By May 2003 the Norton Internet Security has a Macintosh version, *the Norton Internet Security for Macintosh v2.0. Kids GoGoGo* and *KidsServer* which are filtering software only for the Macintosh operating system.[15]

Multi-User Accounts

Multi-user accounts provide various filtering settings for each member of a user group. For instance, with Cyber Patrol parents or administrators can create up to nine accounts with different mixes of twelve filter categories and time schedules. Cyber Snoop and Norton Internet Security provide unlimited multi-user accounts.

Updates

The filter lists are updated daily or weekly by each software company. In my view, considering the growth of the Internet at breakneck speed, daily updating would be preferable. The five products provide daily updated filter lists, including Cyber Patrol, Net Nanny, N2H2, We-Blocker and X-Stop.

Cyber Snoop is the only product that does not provide filter lists by default, while users can request the 'Not Recommended' starter list via e-mail during registration. However, Cyber Snoop provides no further filter update. Users need to build their own filter lists. In reality it seems cumbersome to most end-users. Not many parents can afford to build and update their filter lists. Also, they may not be sufficiently computer-literate to do so. In my view, Cyber

[15] These two software products are made by a Japanese company, MAKI Enterprise Inc. Their free trial versions are available via the company's Website, http://www.makienterprise.com/ (Retrieved May 28, 2003)

Snoop is monitoring software rather than filtering software. As discussed above, of the ten software products, it provides the most impressive performances at reporting, while its filtering function is very poor.

Categories

As the table (Table 4.6) shows, each filter list is classified into a variety of categories. Pure Sight classifies its filter lists into only two categories, sex and gambling. Cyber Sentinel and Cyber Snoop do not provide any information about their filter list categories. In contrast, N2H2 has narrowed down 42 categories, including 36 categories and six exceptional categories. It also offers predefined combinations of filtering categories, called Web content levels; maximum filtering, typical filtering, minimal filtering and no filtering. However, providing more numbers of filter categories does not necessarily mean a better filtering quality, or a better user autonomy. These filter categories are given by private commercial companies which are not obliged to gain any degree of public consent. For instance, when N2H2 filters a Website, it does not provide any information about a category of the blocked site. Thus, a user cannot know why the site is blocked or which category the site falls into. Each product's filter list categories are as follows:

Product	NoC*	Categories
Cyber Patrol	12	Violence/Profanity, Partial Nudity, Full Nudity, Sexual Acts, Gross Depictions, Intolerance, Satanic/Cult, Drugs/Drug Culture, Militant/Extremist, Sex Education, Questionable/Illegal & Gambling, Alcohol & Tobacco
Cyber Sentinel		Unknown
CYBERsitter	5	***Default***: Adult/Sexually Oriented, Illegal Activities/Drugs, Adult/Violence, Hate/Intolerance, Illegal Guns/Violence
	25	***Optional***: Gay/Lesbian Topics, Cults/Occult, Violent Games, Tobacco/Alcohol, Gambling Sites, Banner Ads, Legal Guns/Weapons, Personal Ads, Tattoo/Piercing, Warez/Hacker Sites, On-line Chat, Shareware Sites, Financial Sites, Illegal MP3 Files, Popup Ad Windows, Sports, Game Sites, On-line Auctions, TV/Entertainment, Movie Sites, Wrestling, Job search, Free E-Mail Sites, Pokemon Site, Astrology/Fortune Telling
Cyber Snoop		Unknown
Net Nanny	5	Sexually Explicit, Hate, Violence, Crime, Drugs
Norton Internet Security	31	Adult Humour, Alcohol-Tobacco, Anonymous Proxies, Crime, Drugs/Advocacy, Drugs/Non-medical, Entertainment/Games, Entertainment/Sports, Finance, Gambling, Humour, Interactive/Chat, Interactive/Mail, Intolerance, Job Search, News, Occult/New Age, Prescription Medicine, Real Estate, Religion, Sex/Acts, Sex/Attire, Sex/Nudity, Sex/Personals, Sex Education/Basic, Sex Education/Advanced, Sex Education/Sexuality, Travel, Vehicles, Violence, Weapons
N2H2	36	Adults Only, Alcohol, Auction, Chat, Drugs, Electronic Commerce, Employment Search, Free Mail, Free Pages, Gambling, Games, Hate/Discrimination, Illegal, Jokes, Lingerie, Message/Bulletin Boards, Murder/Suicide, News, Nudity, Personal Information, Personals, Pornography, Profanity, Recreation/Entertainment, School Cheating Information, Search Engines, Search Terms, Sex, Sports, Stocks, Swimsuits, Tasteless/Gross, Tobacco, Violence, Weapons
	6	***Exceptions***: Education, For Kids, History, Medical, Moderated, Text/Spoken Only
Pure Sight	2	Sex, Gambling
We-Blocker	7	Pornography, Violence, Drugs and Alcohol, Gambling, Hate Speech, Adult Subjects, Weaponry
X-stop	34	Alcohol, Alternative Journals, Anarchy, Automobile, Banner Ads, Chat, Criminal Skills, Cults/Gothic, Drugs, Employment, Entertainment, Financial, Free Hosts, Gambling, Games, Hate & Discrimination, Humor, Lifestyle, Magazines, News, Obscene/Tasteless, Opinion/Politics and Religion, Personal/Dating, PG-17, Pornography, R-rated, Search Engines, Self-Help, Shopping, Sports, Tickets, Travel, Web-based E-mail, Web-based Proxies Anonymizers, Web-based Newsgroups

Table 4.6. Filter list categories. * **NoC** = Number of Categories

4.3.6. Effectiveness

For examining the software's filtering effectiveness I tested the products against 200 sample Websites of 10 categories chosen from among ten software's common default filtering categories; Alcohol, Crime, Drugs, Gambling, Gay/Lesbian, Hate/Discrimination, Pornography, Sex, Tobacco, Weapons. A related term of each category (Table 4.7) was entered into the Google search engine, and then the first 20 links generated by the search engine were taken. This resulted in a set of 200 sample Websites.

Category	Keyword	Category	Keyword
Alcohol	Alcohol	Hate	Nazi
Crime	Crime	Pornography	Porn
Drugs	Drug	Sex	Sex
Gambling	Gambling	Tobacco	Cigarette
Gay / Lesbian	Gay	Violence	Gun

Table 4.7. A related term of each category

This test focused on over-blocking sensitivity as well as under-blocking issues, since these two issues have been consistently recognised as one of the major weaknesses of first generation filtering software. The test was conducted between 21st December 2001 and 23rd December 2001 and the results were analysed in January 2002. The list of the sample Websites and the detailed results are in Appendix C.

Category \ Software	CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
Alcohol					1	10			2	
Crime	2					5	4	1	2	1
Drugs						3	1		5	
Gambling	4		18			15	8	19	17	3
Gay / Lesbian	2	2	8		3	15	6	5	16	
Hate	2		1		2	3	7		4	
Pornography	19	20	19	2	11	17	18	15	18	16
Sex	12	6	11	2	12	14	16	8	15	4
Tobacco	1		1		1	8	9		1	
Violence	0		8			11	5		8	
Total	42	28	66	4	30	101	74	48	88	24

Table 4.8. Number of blocked Websites

Notes: ▨ = 0 •=Yes ✘=No **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

As the above table (Table 4.8) shows, the software reviewed mainly focuses on filtering of sex-related information rather than information of other categories. Among the 20 sample sites in the pornography category, 17 sites are genuine pornography sites and the other two sites are anti-child pornography campaign sites; Adult Sites Against Child Pornography (http://www.asacp.org) and Report Child Porn to Government Agencies (http://www.reportchildporn.com). Another site is an un-categorised personal Website. The five products, Cyber Patrol, Cyber Sentinel, CYBERsitter, N2H2, and We-Blocker successfully blocked all pornography sites, although Cyber Patrol, Cyber Sentinel, and CYBERsitter blocked two anti-child pornography campaign sites as well. While Norton Internet Security and We-Blocker covered all ten categories, Cyber Sentinel and Cyber Snoop only filtered Websites in three and two sex-related categories respectively. Norton Internet Security and We-Blocker

blocked 101 and 88 out of 200 sample Websites respectively.

Although Norton Internet Security blocked the largest number of sample Websites throughout all ten categories this does not necessarily mean that it is the best product as the sample Websites are simply collected based on specific keywords and do not represent the entire Internet. Indeed, it was found that of the 101 sites blocked by Norton Internet Security, 17 sites are absolutely legitimate. They include several international organisations and governmental sites. There is even an academic journal site, Alcohol and Alcoholism, which is published by the Oxford University Press which is blocked. The list of over-blocked Websites by Norton Internet Security is as follows (Table 4.9):

Blocked Websites	Category given by Norton Internet Security
The U.S. Bureau of Alcohol, Tobacco and Firearms http://www.atf.treas.gov/index.htm	Alcohol-Tobacco
Alcohol and Alcoholism, Oxford Journals online http://alcalc.oupjournals.org/	Alcohol-Tobacco
Center for Alcohol and Addictions Studies, Brown University, US http://center.butler.brown.edu/	Alcohol-Tobacco
Alcohol Advisory Council of New Zealand http://www.alcohol.org.nz/about/home.html	Alcohol-Tobacco
National Organisation on Fetal Alcohol Syndrome, US http://www.nofas.org/	Alcohol-Tobacco
Fetal Alcohol And Drug Unit, University of Washington http://depts.washington.edu/fadu/	Alcohol-Tobacco
College Alcohol Study, Harvard School of Public Health http://www.hsph.harvard.edu/cas/	Alcohol-Tobacco
Clubdrugs.org –A service of the National Institute on Drug Abuse, US http://www.clubdrugs.org/	Drugs / Advocacy
The Indiana Prevention Resource Center at Indiana University http://www.drugs.indiana.edu/	Alcohol-Tobacco
National Council on Problem Gambling, US http://www.ncpgambling.org/	Gambling
The National Gambling Impact Study Commission, US http://www.ngisc.gov/	Gambling
The Gay Lesbian and Straight Education Network http://www.glsen.org/templates/index.html	Sex Education / Sexuality
International Gay and Lesbian Human Rights Commission http://www.iglhrc.org/	Sex Education / Sexuality
International Lesbian and Gay Association http://www.ilga.org/	Sex Education / Sexuality
The Federation Of Gay Games http://www.gaygames.com/en/	Sex / Acts
SEX.ETC http://www.sxetc.org/	Sex / Nudity Sex Education/advanced
Lung Cancer and Cigarette Smoking http://ourworld.compuserve.com/homepages/LungCancer/	Travel

Table 4.9. Over-blocked Websites by Norton Internet Security

In particular, the Federation of Gay Games, Lung Cancer and Cigarette Smoking Websites are categorised wrongly. The Federation of Gay Games is an international organisation which hosts a quadrennial athletic and cultural event. However, Norton Internet Security classifies the Federation's Website into the Sex/Act category which is defined as "sites depicting or implying sex acts, including pictures of masturbation not categorised under sexual education. Includes sites selling sexual or adult products." Lung Cancer and Cigarette Smoking is an anti-smoking campaign site, but it is classified into a totally unrelated category, namely travel.

Like Norton Internet Security, We-Blocker also poses a serious over-blocking problem. It inappropriately blocks 21 sample sites. It classifies most Websites of International gay/lesbian organisations into the pornography category. Even an anti-Internet censorship article site, 'Sex, Censorship, and the Internet' is categorised as a pornography site. The list of over-blocked Websites is as follows (Table 4.10):

Blocked Websites	Category given by We-Blocker
The National Clearinghouse for Alcohol and Drug Information, US http://www.health.org/	Drugs and Alcohol
Internet Alcohol Recovery Center, University of Pennsylvania http://www.uphs.upenn.edu/~recovery/	Adult Content Drugs and Alcohol
Clubdrugs.org (A service of the National Institute on Drug Abuse) http://www.clubdrugs.org/	Drugs and Alcohol Pornography
Stop drugs http://www.stopdrugs.org/	Drugs and Alcohol
The National Institute on Drug Abuse, US http://www.nida.nih.gov/DrugAbuse.html	Drugs and Alcohol
The U.S. Drug Enforcement Administration http://www.usdoj.gov/dea/concern/concern.htm	Drugs and Alcohol
The National Criminal Justice Reference Service / Drugs And Crime http://virlib.ncjrs.org/DrugsAndCrime.asp	Drugs and Alcohol
The Gay Lesbian and Straight Education Network http://www.glsen.org/templates/index.html	Pornography Adult Content
The Gay & Lesbian Alliance Against Defamation http://www.glaad.org/org/index.html	Adult Content
Gay Men's Health Crisis http://www.gmhc.org/	Pornography Adult Content
The International Gay and Lesbian Human Rights Commission http://www.iglhrc.org/	Pornography Adult Content
The International Lesbian and Gay Association http://www.ilga.org/	Adult Content
The Federation Of Gay Games http://www.gaygames.com/en/	Pornography
The National Lesbian & Gay Journalists Association http://www.nlgja.org/	Pornography Adult Content
Gay-Lesbian Politics and Law WWW and Internet Resources http://www.indiana.edu/~glbtpol/	Pornography Adult Content
SEX ETC. The Network for Family Life Education, Rutgers University, US http://www.sxetc.org/	Pornography Drugs and Alcohol
Sex, Censorship, and the Internet http://www.eff.org/CAF/cafuiuc.html	Pornography
Stop Sex Offenders! http://www.stopsexoffenders.com/	Pornography
All About Sex Discussion Web http://www.allaboutsex.org/	Adult Content
The Sex Education Web Circle http://www.sexuality.org/wc/	Adult Content
Fact Sheet – Cigarette Smoking http://www.well.com/user/woa/fssmoke.htm	Pornography

Table 4.10. Over-blocked Websites by We-Blocker

In contrast to Norton Internet Security and We-Blocker which over-block many legitimate sites, Cyber Snoop omits too many Websites which may be harmful to minors. Throughout all categories the Cyber Snoop's performance is very disappointing. In total it blocks only four sites, including two pornography sites, one safe sex campaign site and one anti-Internet censorship article, while it omits 15 pornography sites. Similarly, X-stop omitted most gambling sites. Cyber Sentinel, Cyber Snoop, and Net Nanny did not block any gambling sites at all. Surprisingly, no software blocked the Website of the Libertarian National Socialist Green Party (http://www.nazi.org) – in my view, this is reflection of the US political standard. Neo-Nazi activities are constitutionally protected in the US, while any neo-Nazi propaganda is illegal in many European nations, such as Germany and the Netherlands.

Overall, some degree of over and under-blocking frequently occurred through all the filtering software products I reviewed. Since filtering software has been designed and developed mainly for protecting minors from inappropriate information on the Internet, theoretically it is expected to filter explicit pornographic information, while it provides a free flow of a vast amount of healthy information on the Internet – as mentioned above, the result of my test confirms that filtering software mainly focuses on filtering of sex-related information rather than information of other categories. In practice, however, it under-blocks a number of explicit pornography Websites, while it unnecessarily over-blocks a significant number of Websites which do not contain any obscene information. Moreover, many sites are initially classified into irrelevant categories. In my view, these technical shortcomings of the first generation filtering software products are incurable, since the filtering technologies which they employ, such as URL-based filtering and keyword-based filtering, have inherent weaknesses which will be discussed in the next section. Consequently, the software's effectiveness is unreliable, although some

products performed well in the pornography category.

4.4. A Critique of First Generation Filtering

The first criticism that can be levelled against first generation filtering is that it restricts user autonomy. As reviewed above, most types of filtering software allow a user-defined control. Users can choose certain categories of filter lists. Furthermore, users are allowed to modify the filter lists. Indeed, most filtering software provide various user-customised options.

However, in my opinion, this does not mean that filtering software really provides user autonomy. Their user-customised options are burdensome and limited. First of all, most of their filter lists are not transparent. Although users can manually add or delete a site or word from filter lists one by one, the remaining thousands of blocked Websites and keywords in the filter lists are still unknown. Thus, users cannot know what their filtering software is blocking in practice. In the case of server-side filtering which is usually employed by ISPs, user autonomy may be far more restricted. It would mean that users' rights to choose certain Internet information are virtually in commercial companies' hands. In my view, the responsibility for deciding what is harmful and what is not should rest with individuals, not with commercial companies. In terms of child protection, Cyber-Rights & Cyber-Liberties (1997) argues that the prime responsibility for protecting children from accessing pornographic content should not be put on the filtering software industry, but on parents and teachers. An Internet activist, Declan McCullagh,[16] said, "Filtering software is a classic case of a privatised censorship scheme." (Aguilar, 1996) Indeed, most filtering software companies hold their databases

[16] Declan McCullagh was the Washington bureau chief for Wired News from 1998 to 2002. He is the chief political correspondent for CNET's News.com.

of blocked sites as proprietary information, because the greatest commercial value of filtering software consists in blocking databases. For this reason, of the ten software reviewed, only two products, Cyber Snoop and Net Nanny, provide transparent filter lists (see Chapter 4.3.4).

However, even if all filtering software made their filter lists viewable, this problem might still not be solved. Because a filter list contains hundreds of thousands of Web pages – by May 2003 Cyber Snoop provides its un-encrypted block list which contains 14,719 URLs – and is constantly updated, only few parents may be capable of reviewing the entire list, and then customising it. According to a product manager for Compuserve's software package, 'Internet in a Box for Kids,'[17] Kevin Britt, "Parents don't want to know about configuration settings, they just want the stuff to work." (O'Brien, 1996) Moreover, most filtering software fails to give users any explanation as to why they block a site. Of the ten software packages reviewed, only Norton Internet Security and We-Blocker simply indicate a category of blocked sites. Another problem concerns the filtering criteria, which are provided by filtering software companies, but are never publicly discussed. It depends entirely on private commercial companies whether the criteria are appropriate or not.

The second criticism to be levelled at first generation filtering is that it continuously and inevitably raises issues concerning under-blocking and over-blocking. As confirmed through the test above, many filtering software frequently omit to block some potentially harmful Internet sites. The Online Policy Group (2001)[18] argues that:

---

[17] 'Internet in a Box for Kids' was a one-box Internet-access package designed for children aged 8 to 14.

[18] The Online Policy Group is a US-based non-profit organisation dedicated to online policy research. It was founded by Will Doherty in July 2000. Currently, it is based in San Francisco. Its Website address is http://www.onlinepolicy.org/ (Retrieved October 9, 2004).

> No blocking technology is clever enough to block even 10% of the pornography on the Internet unless it effectively blocks most or all of the materials on the Internet.

The quantity of information on the Internet is simply too vast. More than seven million new Web pages are added each day (Cyveillance, 2000). Even the world-class search engines reflect only a fraction of content available on the Internet.[19] It is impossible for filtering software to evaluate all content available on the Internet. Thus, under-blocking is an unavoidable weakness of filtering software. According to a report from *Consumer Reports* (2001),[20] Cyber Patrol failed to block 23 percent of objectionable sites. CYBERsitter, Net Nanny and Norton Internet Security also failed to block respectively 22, 52 and 20 percent of sites deemed harmful.

Alongside under-blocking issues, over-blocking raises controversy regarding freedom of expression on the Internet. Filtering software blocks not only harmful Internet sites, but also many controversial and even non-controversial sites. They block sites that contain information relating to gay, lesbian and feminist issues. Even health campaign sites are blocked. For instance, Internet sites concerning AIDS information and education for safe sex, which might be accessed by a wide range of people including teenagers, are blocked by many commercial filtering products. According to a report by the Kaiser Family Foundation (2002), *See No Evil: How Internet Filters Affect the Search for Online Health Information*, one in three "safe sex" health sites are blocked by at least one of the filters, which the Foundation tested, even when set at their

---

[19] According to research, search engine coverage relative to the estimated size of the publicly indexable web has decreased substantially since December 1997, with no engine indexing more than about 16 percent of the estimated size of the publicly indexable Web (Lawrence & Giles, 1999).

[20] Consumer Reports is a magazine which is published by the Consumers Union in the US. The magazine was first published in 1936.

least restrictive settings. In addition, some filtering software companies are using their products to suppress criticism of them; for instance, I found that CYBERsitter blocks Peacefire.org[21] and Censorware Project's[22] Websites which criticise filtering software. The Commission on Child Online Protection (2000, p. 19)[23] also highlighted this issue through its final report in October 2000 as follows:[24]

> This technology raises First Amendment concerns because of its potential to be over-inclusive in blocking content. Concerns are increased because the extent of blocking is often unclear and not disclosed.

The third point of critique of first generation filtering is that the filtering software cannot understand the various contexts in which information appears. Heins and Cho (2001) point out that the problem of Internet content filtering stems from its nature, which largely relies on mindless mechanical blocking through identification of key words and phrases. Many sites are blocked by keyword filtering which relies on researching only isolated indecent words. For instance, if a filtering software product is set to block sites which contain the word, 'breast', sites which contain a recipe for chicken breast or medical information concerning breast cancer will be blocked by the filtering product.

---

[21] Peacefire.org was created in August 1996 to represent the interests of people under 18 in the debate over freedom of speech on the Internet. The first content to appear on Peacefire.org consisted of lists of some of the Websites that were blocked by popular filtering programmes such as Cyber Patrol and CYBERsitter. Since then, the information on Peacefire.org has been used by lawyers for the ACLU and other anti-censorship groups to challenge Internet censorship.

[22] One of famous anti-censorship campaign Websites, the Censorware Project was formed by a group of writers and internet activists in late 1997.

[23] The Commission, a congressionally appointed panel, was mandated by the Child Online Protection Act, which was approved by US Congress in October 1998.

[24] The full text of the Commission's final report is available at http://www.copacommission.org/report/COPAreport.pdf (Retrieved May 29, 2003)

Although this may be an extreme example, in my view, other similar situations may easily occur with any other word or phrase, such as drug and sex. In this sense, keyword filtering cannot relate the words to their broader context, because "context is simply too complex for mechanical evaluation." (Balkin & Roosevelt, 2000) No matter how filtering technology is improved it can never understand the complexity of human language. Furthermore, keyword filtering faces serious multilingual issues. The Internet is a global medium which contains information in hundreds of different languages, although the Internet is still an English-dominant environment. For instance, there can be hundreds of different non-English expressions or slang words which mean 'bestiality.' A bestiality picture file which has a non-English name can be available on the Internet. It may not be blocked by English-based filtering products, unless those filtering products cover all those various non-English languages.

4.5. Free Speech Rights Issues of Filtering Software on the Internet

Internet content filtering software has led to intense debate among civil liberties groups, such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF). They deem this to be censorship. Ann Beeson, an ACLU staff attorney,[25] said, "Blocking software is nothing more than CDA in a box." (Clausing, 1998) One of the campaign groups against filtering, Nofilters.org (2000),[26] argues that:

> Filtering is a process whereby somebody's access to Internet content is censored by parents, an institution, an employer, or the state. This censoring (filtering) is usually achieved via technological means such as a software product. In most cases, the

[25] Ann Beeson is a staff counsel at the ACLU National Headquarters in New York City. As counsel for the plaintiffs in *ACLU v. Reno*, she is a primary architect of the CDA case.

[26] http://www.nofilters.org

> stated objective is to "protect" children [...] from what the proponents define as smut or pornography on the Internet.

The ACLU and the EFF argue that the first generation Internet filtering technologies are simply unworkable because they have inherent weaknesses – this issue will be discussed later in the chapter in depth. They are critical of the fact that most commercial filtering software has violated free speech rights and will eventually wipe out minor and controversial, yet innocent incidences of free speech on the Internet.

In this context, the UK Internet industry's 'R3 Safety-Net' approach stresses the promotion of PICS-based rating systems (see Chapter 3.6.1). In September 2001 the Council of Europe (2001b) adopted recommendations concerning Internet content self-regulation that strongly endorses Internet content labelling systems which are applied by users on a voluntary basis — in Chapter 5, I will discuss PICS in depth.

However, unlike in Europe, first generation filtering has become a major issue in the US. Firstly, two previous criminal laws against distribution of "indecent" information for minors on the Internet, *the Communication Decency Act* (CDA) (see Chapter 2.6.1.1) and *the Child Online Protection Act* (COPA) (see Chapter 2.6.1.2), have led many software publishers to develop various filtering products. As a result, most popular filtering products in the current market, such as Cyber Patrol, Cyber Sitter, and N2H2, are produced by US-based companies. Secondly, alongside the booming filtering software market, the US government has introduced a law, named *the Children's Internet Protection Act* (CIPA) that makes mandatory the installation of filtering software in schools and libraries. Thus, it is highly noticeable that while Internet content regulations have been strongly driven by the government and

Congress in the US, many European governments, including the UK government and the EU, prefer co-operative regulation which is jointly conducted by the Internet industries, governments, and end-users as opposed to heavy-handed governmental regulation.

In this sense, it is necessary to discuss US legal cases that deal with filtering software issues. The next section will explore a legal battle over the CIPA, because it is the mandated filtering law that forces public institutions to use technical measures, mainly first generation filtering software. However, before this case is discussed, a previous case, *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, Virginia*, will be examined since this is the first case that directly addressed issues concerning a public library's mandatory Internet filtering policy.

4.5.1. Case Study: Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, Virginia, 1998

Loudoun County is located in far northern Virginia. It is the home of many major computer and Internet companies, such as American Online and UUNet. The County runs a public library system with six branches.

In October 1997 the Board of Trustees of the Loudoun County Public Library passed a "Policy on Internet Sexual Harassment" that was designed to prevent "creating a sexually hostile environment and violating obscenity, child pornography, and harm to juveniles laws." The Library Board was concerned that Internet viewing might lead to a sexually hostile environment without installing filtering software. The policy stated the following restrictions on the

library's Internet access service:[27]

> (1) E-mail, chat rooms, and pornography will not be provided; (2) Site-blocking software (software that blocks by specific site, rather than by suspect-word category) will be installed on all computers. To the extent technically feasible, such software will: (a) block child pornography and obscene material (hard core pornography); (b) block material deemed harmful to juveniles under applicable Virginia statutes and legal precedents (soft core pornography). Public access to such material could create an unlawful, sexually-hostile environment, and might incite dangerous criminal misconduct. (3) Internet computers will be installed in close proximity to, and in full view of, library staff in order to: (a) discourage efforts to override the blocking software; and, (b) provide patrons a secure environment against sexual harassment when using the Internet. (4) Patrons will not be permitted to use the Internet to access pornography. Persons using the Internet to access material in paragraph 2, will be told they are violating the Policy on Internet Sexual Harassment. If they continue, they will be told to leave the library. If they refuse, they will be considered in trespass, and police may be called to remove them. Children's parents will also be notified unless the child obeys the first request to stop.

To fulfill the second restriction the library purchased the commercial filtering product manufactured by Log-On Data Corporation, the library edition of the X-Stop.[28] However, this policy immediately faced a legal challenge by a Loudoun County non-profit organisation, Mainstream Loudoun, and its individual members, who were residents of Loudoun County (*Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, No. 97-2049-A). The plaintiff group argued that:

---

[27] The full text of the policy is available at the Mainstream Loudoun's Website, http://www.loudoun.net/mainstream/Library/summintpol.htm (Retrieved May 25, 2003)

[28] X-stop was one of the first commercial filtering software to be available not only for personal computers, but also for networks and proxy servers. It has been on the market since 1995.

> [...] the library Internet use policy and filtering software improperly limit adults to even less information than is fit for children, block access to valuable, educational, and constitutionally protected information that has nothing to do with sexually explicit materials, fail to promote purported objectives, and ignore readily available less-restrictive alternatives (Krug, Matthew & Robinson, 1998).

On 7th April 1998, Judge Leonie M. Brinkema of the US District Court for the Eastern District of Virginia rejected a government motion to dismiss the case. The judge said that the defendants had "misconstrued the nature of the Internet" and held that "the Library Board may not adopt and enforce content-based restrictions on access to protected Internet speech [in the absence of] a compelling state interest and means narrowly drawn to achieve that end."[29] In the Court's final decision, made on 23rd November 1998, Judge Brinkema concluded as follows:

> [The policy] (1) is not necessary to further any compelling government interest; (2) is not narrowly tailored; (3) restricts the access of adult patrons to protected material just because the material is unfit for minors; (4) provides inadequate standards for restricting access; and (5) provides inadequate procedural safeguards to ensure prompt judicial review.[30]

The judge ruled that such a policy offends the guarantee of free speech in the First Amendment and is, therefore, unconstitutional. Judge Brinkema held that the library falls into a category known as a "limited public forum," because one

---

[29] The full text of this decision is available at Tech Law Journal's Website, http://www.techlawjournal.com/courts/loudon/80407mem.htm (Retrieved May 21, 2003)

[30] The full text of this ruling is available at the EFF's Website, http://www.eff.org/Legal/Cases/Loudoun_library/HTML/19981123_opinion_order.html (Retrieved May 21, 2003)

of its missions is "receipt and communication of information through the Internet." The judge also pointed out that it is undisputed that the filtering software does not base its blocking decisions on any legal definition of obscenity. The Censorware Project[31] (2000) argues in its article, *Loudoun County, VA Censorware Lawsuit*, "the librarian should not delegate decision making about the appropriateness of content to a private company using vague, undisclosed standards." The Library Board decided not to appeal in April 1999. Although it was a district court's decision, this case is significant because it set a judicial precedent for Internet access in public libraries across the US. It also strongly influenced another similar case, the Children's Internet Protection Act (CIPA) case, which will now be discussed.

4.5.2. Case Study: The Children's Internet Protection Act, 2000

As mentioned above, unlike many European governments, the US government and Congress have introduced mandated filtering law nationwide. *The Children's Internet Protection Act*, the so-called CIPA, is a prime example.

This was initially introduced by four Republican Senators; John McCain, Rick Santorum, Ernest Istook, and Charles Pickering in January 1999 and signed into law on 21st December 2000 by President Clinton. The CIPA enforces public libraries' and schools' installation of filtering software on all of their computers which provide Internet access. Under the CIPA no public library or school may receive federal grants unless it certifies that it adopts and implements an Internet safety policy which includes use of a "technology protection measure" that would block or filter three classes of visual depiction: obscenity, child pornography and material deemed to be harmful to minors

[31] The Censorware Project was formed by a US-based group of writers and internet activists in late 1997 (Resource: Censorware Project Website. Retrieved March 26, 2005, from http://censorware.net/).

(CIPA Sec.1711). The CIPA does not target text format information.[32]

If public libraries or schools fail to comply with the CIPA, they will lose the Federal Communications Commission's discount on telecommunications and Internet-related technologies, known as E-rate. Moreover, they will lose federal grants which are made under *the Library Service and Technology Act* (LSTA)[33] and *the Elementary and Secondary Education Act* (ESEA).[34] "Public libraries annually receive grants 65 million USD in discounts and 150 million USD in grants." (Industry Standard, 2001) According to the American Library Association[35] (ALA, 2002), during the four years from 1999 to 2002, under the federal E-rate programme, more than 255.5 million USD had been disbursed to more than 5,000 public libraries. Since 1998, the LSTA has offered more than 883 million USD to libraries nationwide. It is inevitable that

---

[32] The Full Text of Legislation (Title XVII of H.R. 4577) is available at http://www.merit.edu/usf/CIPA.html (Retrieved May 26, 2001).

[33] The Library Service and Technology Act (LSTA) enacted on 30th September 1996. According to the ALA, the purpose of LSTA is as follows:

> [To] consolidate Federal library service programs; to stimulate excellence and promote access to learning and information resources in all types of libraries for individuals of all ages; to promote library services that provide all users access to information through State, regional, national and international electronic networks; to provide linkages among and between libraries; and to promote targeted library services to people of diverse geographic, cultural, and socioeconomic backgrounds, to individuals with disabilities, and to people with limited functional literacy or information skills (ALA Washington Office, 1996).

[34] The Elementary and Secondary Education Act (ESEA) is the US government's single largest investment in elementary and secondary education. It provides targeted resources to help ensure that disadvantaged students have access to a quality public education. ESEA was originally authorised in 1965 for five years and had been reauthorised every five years since. (Resource: National Education Association, US. Retrieved 25th October, 2004, from http://www.nea.org/aboutnea.html)

[35] The ALA is a professional body of librarians in the US which was founded in 1876. Its mission is "to provide leadership for the development, promotion, and improvement of library and information services and the profession of librarianship in order to enhance learning and ensure access to information for all." Its membership is open to "any person, library, or other organisation interested in library service and librarianship [...]" (Resource: ALA Website. Retrieved March 15, 2004, from http://www.ala.org/ala/ourassociation/ourassociation.htm)

most public libraries across the US acquiesce in the CIPA because they largely depend on these federal grants.

Nevertheless, in March 2001 the ALA filed a legal challenge to the CIPA, *United States vs. CIPA,* in a district court in Philadelphia. The ACLU also instituted a separate legal challenge on behalf of public libraries, library patrons and Website authors.[36] This case is *Multnomah County Public Library*[37] *vs. United States*. Multnomah County Library and other plaintiffs were represented by the ACLU. Both suits targeted two institutions which are charged with enforcing the CIPA; the Institute of Museum and Library Service[38] and the Federal Communications Commission.[39] The ALA and the ACLU argued that requiring libraries and schools to install filtering software is de facto censorship and that the CIPA violates free speech rights which should be protected by the First Amendment. Moreover, they criticised the CIPA for discriminating against people who rely on schools and libraries for their Internet access, because those people would be forced to access only filtered information whether they want to or not (Bowman, 2001). ALA President,

---

[36] The ACLU's plaintiffs consisted of not only a group of librarians, but also library patrons and Website authors. The library patrons ranging from a 16-year-old college student to a doctoral candidate testified to their experience at public libraries. Websites which provide sexual health information, such as AfraidtoAsk.com and Safesex.org, joined with the plaintiffs (ACLU, 2001).

[37] Multnomah County Public Library is a department of Multnomah County, Oregon, US that provides library services through the Central Library and fifteen branches in the Portland, Oregon metropolitan area.

[38] The Institute of Museum and Library Service is an independent US government agency that supports all types of museums, from art and history to science and zoos, and all types of libraries and archives, from public and academic to research and school.

[39] The Federal Communications Commission (FCC) is an independent US government agency, directly responsible to Congress. The FCC was established by *the Communications Act* of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the fifty states, the District of Columbia, and US possessions.

Nancy Kranich stated that:

> Forcing libraries to choose between funding and censorship means millions of library users will lose—particularly those in the most poverty-stricken and geographically isolated areas of the country. [...] The federal government should not be subsidising commercial filtering companies by forcing libraries to buy technology that doesn't work (ALA, 2001).

The two cases were consolidated by the court and were heard together by a three-judge panel in a federal district court in Pennsylvania, chief judge Edward R. Becker and district judge John P. Fullam and Harvey Bartle III. In May 2002 the three-judge panel ruled that the CIPA is unconstitutional.[40] The court decided that Sections 1712(a)(2) (codified at 20 U.S.C. §9134(f)(3)) and 1721(b) (Codified at 47 U.S.C. §254(h)(6)) of the CIPA, which define "limitation on availability of certain funds for libraries" and "requirements for certain libraries with computers having Internet access" respectively, are invalid under the First Amendment and enjoined the government not to enforce those provisions. The Court said that:

> [...] we are constrained to conclude that the library plaintiffs must prevail in their contention that CIPA requires them to violate the First Amendment rights of their patrons, and accordingly is [...] invalid, even under the standard urged on us by the government, which would permit us to [...] invalidate CIPA only if it is impossible for a single public library to comply with CIPA's conditions without violating the First Amendment. In view of the limitations inherent in the filtering technology mandated by CIPA, any public library that adheres to CIPA's conditions will necessarily restrict patrons' access to a substantial amount of protected speech, in violation of the First Amendment (*United States v. ALA*, 201 F. Supp. 2d 401).

---

[40] The full text of the decision is available at http://www.paed.uscourts.gov/documents/opinions/02D0415P.HTM (Retrieved May 26, 2003)

The case went to the US Supreme Court. In June 2003 the Court reversed the federal panel's decision and declared the CIPA constitutional in a 6-3 ruling. The Supreme Court concluded that:

> Because public libraries' use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power. [...] Concerns over filtering software's tendency to erroneously "overblock" access to constitutionally protected speech that falls outside the categories software users intend to block are dispelled by the ease with which patrons may have the filtering software disabled (*United States v. ALA,* 539US (2003), No. 02-361).

Despite the Supreme Court's ruling, the ALA (2003) announced that:

> We continue to oppose the use of filters that block access to constitutionally protected speech and believe filters are not the best way to ensure library users have a safe and enriching online experience.

Sobel (2003)'s[41] criticism is that:

> The Court assumed that librarians would automatically and unconditionally disable filters upon request by adult patrons and permanently unblock erroneously blocked sites. This assumption puts the burden of ensuring access to constitutionally protected speech upon librarians through a process that is complex and uncertain at best. Furthermore, the Court failed to confront the privacy implications and practical difficulties of such a disabling scheme.

Consequently, in spite of many criticisms, according to the Supreme Court's

[41] David L. Sobel is a general counsel of the Electronic Privacy Information Center.

decision, public libraries and schools in the US are now installing Internet content filtering software. By 1st July, 2004 they will have to comply with the CIPA requirements to receive E-rate funding in the fiscal year 2003.

As discussed in the previous chapters, the prime responsibility for controlling harmful content lies with users, while illegal content is a matter of law-enforcement authorities. In this context, Internet content filtering software is initially designed to prevent individual users from accessing harmful content which they do not want. It cannot be a mandatory tool for controlling harmful content. This mandatory filtering legislation can be compared with the BSA 1999 in Australia. As mentioned in Chapter 2, the Australian government introduced a provision which articulates that an industry code should deal with "alternative access-prevention arrangements" for end-users. (Article 60 of BSA, see Chapter 2.6.2.1). In response to the provision, an industry Code of Practice was developed and approved by the ABA which required ISPs to provide filtering software to users. Despite all these provisions and codes, the final decision lies with users who are not legally required to use filtering software that is offered by an ISP (EFA, 2002a).

I have no objection to parents deciding to use commercial filtering software at home for their own children, as long as they are aware of its limitations. However, installing mandatory filtering software at public Internet access points, such as public libraries and Internet cafés, is a different case, as it may breach people's rights to access certain information. The ALA Intellectual Freedom Committee (2000) states that filtering products have created "a dissonance with the basic mission of libraries." It claims, "Libraries are responsible for serving a broad and diverse community with different preferences and views. Blocking Internet sites is antithetical to library missions because it requires the library to limit information access."

4.6. Conclusion

In summation, no filtering software is entirely accurate and reliable. They frequently fail in their mission which is to restrict children's access to harmful information on the Internet effectively. They also infringe users' autonomy. Although most filtering software allows user-defined control, it never provide real freedom for accessing and speaking on the Internet. Users are able to enjoy only freedom of choice under the limitation that is offered by filtering software producers.

Nevertheless, advocates including many parents and organisations such as the Childnet International[42] and the Internet Watch Foundation, seem to think that these filtering software products are better than nothing. As mentioned above, the filtering software products are widely used in homes, schools, and even libraries and they are gaining in popularity. One of the CIPA's authors, Ernest Istook, argues that blocking some legitimate information is a price worth paying to protect minors from unwanted information on the Internet. He said, "Filters will never be perfect, but that is no excuse not to try to protect our children." (Das & Pike, 2001)

However, in my view, these ideas give rise to serious problems. First of all, the serious shortcomings of filtering software are not temporary, but inherent. Why should free speech rights be restricted because of the imperfection of filtering technologies? "Freedom of expression is a thing of great value which must not be compromised by efforts to achieve a safe Internet." (Economic and Social Committee of the European Commission, 1998) Moreover, there is a risk that

[42] The Childnet International is a UK-based non-profit organisation with the mission to "work in partnership with others around the world to help make the Internet a great and safe place for children." It was set up in 1996 (Resource: Childnet International Website. Retrieved June 2, 2003, from http://www.childnet-int.org/about/index.html).

parents will put excessive confidence in commercial filtering software, since most commercial filtering product companies are unlikely to inform end-users that their products have inherent technical limitations, whereas they are quick to advertise how brilliant their products are. In other words, the use of filtering products may give parents and teachers a false sense of security. The Economic and Social Committee of the European Commission states the following in its report:

> A danger of this technological approach is that, once a filter system has been installed, parents and teachers, believing that their children are now in a safe environment, will see no need for further supervision, not realising that children will quickly find any loopholes in the system. Experience has shown that children's computer knowledge often surpasses that of their parents and teachers (Economic and Social Committee of the European Commission, 1998).

In this context, the Internet Watch Foundation states that parents and teachers should be aware of filtering software's technical weaknesses and limitations:

> [T]he most important thing to remember when it comes to considering which tools to use is that no single filtering product can be guaranteed to totally protect your child from accessing inappropriate material. [...] Like a seat belt in a car, a filter can help protect you but it cannot guarantee you will not have a crash! (IWF, 2003b)

The first generation filtering products may be useful in some limited environments, such as the primary school classroom. Also, it may help to limit the potential dangers to children on the Internet. However, its inherent drawbacks overwhelm its advantages. Benjamin Edelman (2001) argues that the flaws of filtering software are fundamental. He states, "blocking programmes are fundamentally unable to block all Internet content that meets

specific category definitions while simultaneously allowing access to all other content." As the Kaiser Family Foundation (2002) reported, Internet filters may reduce, but do not prevent, children from inadvertent exposure to harmful content. While they make it substantially harder for young people to proactively seek out pornographic content, they do not entirely prevent it. The above reasons mean that I cannot recommend the use of commercial filtering software.

Although the US Supreme Court ruled that installing filtering software is constitutional through the CIPA case, criticisms on that decision from many organisations, such as the ALA, still remain. It should be emphasised again that technical weaknesses of filtering software are inherent and cannot be improved. Therefore, it is doubtful that installing filtering software in public libraries and schools will have the positive effect that the US Congress expects. In this context, one of the EU Action Plan's, to develop filtering and rating systems, is also doubtful.

In the following chapter another filtering system, the PICS-based label filtering system, which has been referred to as an alternative to first generation filtering, will be discussed. Its technical specification will be explored and its drawbacks and advantages will be examined in depth.

CHAPTER 5

THE INTERNET CONTENT RATING SYSTEM

5.1. Introduction

As discussed in the previous chapter, first generation filtering software poses a number of serious problems none of which are likely to be solved in the foreseeable future. In a sense, the Internet content rating system has been developed as an alternative. Furthermore, it has been endorsed as a technical solution for preventing children from accessing harmful Internet content by a number of Internet self-regulatory bodies and governments such as the Internet Watch Foundation and the EU. The 'Action Plan on Promoting Safer Use of the Internet' has supported the development of an International Internet content rating sytem taking into account Europe's cultural and linguistic diversity (European Commission, 1999a, p. 3). In this chapter the technical aspects of the Internet content rating system will be explored and three leading rating systems, SafeSurf, RSACi and ICRA, will be examined. The advantages and disadvantages of the Internet content rating system will also be discussed.

5.2. Internet Content Rating System: Technical Specifications

5.2.1. PICS

In discussing any issue relating to the Internet content rating system, it is necessary to begin by mentioning the Platform for Internet Content Selection (PICS), since it is the dominant standard for label filtering. PICS was developed as a set of software specifications for label formats and distribution methods by W3C with the participation of many companies, organisations and institutions.[1] W3C (1997a) defines it as follows:

[1] Apple, America Online, AT&T, the Centre for Democracy and Technology, CompuServe, DEC, IBM, MCI, the MIT Laboratory for Computer Science, Microsoft, Netscape, Prodigy,

> The PICS specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy.

In August 1995, the development of technical specifications was launched. In early 1996, the final technical specifications were completed (W3C, 1998). Since then, PICS has swiftly caught on with the Internet industry. Several PICS-based rating services have been developed, including RSACi and SafeSurf. Moreover, a number of stand-alone filtering software packages have become PICS-compliant.[2] Microsoft Internet Explorer (IE), which currently dominates the Web browser market all over the world, is compatible with PICS. Consequently, most Internet content rating services today follow the PICS specifications.

PICS was designed to provide a technical standard for creating, distributing and using metadata.[3] Associated with a certain URL, PICS equips various people and organisations to create labels which can provide any kind of descriptive information about Internet content, including the rating information. For instance, if a Web page contains an article which is appropriate only for adults, a label might include the statement that there is a certain type of adult information on the page – labelling can be done either by first-party or by third-party. I will discuss the detailed process of labelling later in this chapter. In other words, PICS is a technical standard for dealing with labels of Web

---

the Recreational Software Advisory Council, SafeSurf, SurfWatch, Time Warner Pathfinder and others took part in developing PICS (Resnick & Miller, 1996).

[2] Among ten filtering software products which are reviewed in Chapter 4, five products support PICS-based rating system. The products are Cyber Patrol, CYBERsitter, Cyber Snoop, Net Nanny and Pure Sight.

[3] Metadata is information about information. However, in the PICS context it can be defined as machine-readable information that describes content in an HTML document.

documents at certain URLs. The general form for a label list is as follows (Miller, 1996):

```
(PICS-1.1
    <service url> [option...]
    labels [option...] ratings (<category> <value> ...)
    labels [option...] ratings (<category> <value> ...)
    ...
    <service url> [option...]
    labels [option...] ratings (<category> <value> ...)
    labels [option...] ratings (<category> <value> ...)
    ...
...)
```

For instance, the syntax of the RSACi's label for Playboy online magazine is as follows:

```
<META http-equiv="PICS-Label"
content='(PICS-1.1 "http://www.rsac.org/ratingsv01.html"
l gen true comment "RSACi North America Server" by "eileenk@playboy.com"
for "http://www.playboy.com" on "2000.08.19T09:30-0500"
r(n 4 s 3 v 0 l 4))'>
```
[4]

Each element of this syntax means as follows (Table 5.1):

[4] This syntax is retrieved on 10th May 2000 from Playboy Website, http://www.playboy.com

<META http-equiv="PICS-Label"		The character of the meta tag
PICS-1.1		The current version of PICS
http://www.rsac.org/ratingsv01.html		The URL of the rating service
Labels [option]	l	Label
	Gen	Generic Boolean: If this option is set up as 'true', all URLs which start with 'for quoted URL' are applied at the same rate.
	Comment	Information for people who read the label.
	by "name"	The people or department responsible for creating the label.
	for "URL"	URL which is rated
	On	Date of rating on year . month . day . time : hour . minute. ('+' or '-') sign of time zone offset from UTC[5] amount of offset from UTC
Ratings (<category><value>)		Rating information of each category n = nudity, s =sex, v = violence, l = language. n 4 = Frontal nudity s 3 = Non-explicit sexual acts v 0 = None of the above or sport related l 4 = Crude, vulgar language or extreme hate

Table 5.1. The syntax of the RSACi's label

Balkin, Noveck, and Roosevelt (2000, p. 220), members of the Information Society Project at Yale Law School,[6] said, "Strictly speaking, PICS itself is not a rating system." Indeed, PICS does not rate anything nor provide a specific rating criterion. It merely gives an outline of the basic format for

[5] Coordinated Universal Time

[6] Jack M. Balkin is a professor at Yale Law School and a director of the Information Society Project. Beth Simone Noveck is a International Programmes director of the Information Society Project. Kermit Roosevelt is a resident fellow of the Information Society Project.

labelling. Thus, for the implementation of the PICS specifications, a certain rating and labelling service and PICS compatible filtering software are essential. Resnick (1999)[7] lists six major tasks of this implementation that can be operated by various parties as follows:

1. Set labelling vocabulary and criteria for assigning labels
2. Assign labels
3. Distribute labels
4. Write filtering software
5. Set filtering criteria
6. Install/run filtering software

Firstly, to establish an Internet content rating system, the development of a standard vocabulary and categories for labels are required. Here, the term "vocabulary" means any description of Internet content. For instance, RSACi rates Web content in four categories: violence, nudity, sex, and language. Each category's vocabulary elements, so-called descriptors, are assigned scalar values from zero to four. The sex category includes the following descriptors: "Level 1—Passionate kissing," "Level 2—Clothed sexual touching," "Level 3—Non-explicit sexual acts" and "Level 4—explicit sexual acts or sex crimes." If Microsoft IE adjusts the rating level of the sex category to Level 2, it will block Web pages which are rated as level 3 or 4 of this category (Fig. 5.1). The filter setting of Microsoft IE does not seem to be easy to access for some parents who are not computer-literate, since it is hidden several layers down in the main menu rather than appearing in the top menu. Fortunately, the RSACi system has been adopted by Microsoft IE as a default feature. In other rating systems users have to manually install a "RAT" file[8] on their Web

[7] Paul Resnick is an associate professor at University of Michigan. He chaired the PICS Interest Group at W3C and was one of the main authors of the PICS technical specifications.

[8] RAT file is a text file with a filename suffix of ".rat" which contains a description of a rating system.

browsers. For instance, in the case of the SafeSurf system in order to use the system in Microsoft IE users need to download "SafeSurf.rat" file from the SafeSurf Website and then save that file in the Windows/System32 folder or WINNT/System32 folder. This matter is, in my view, directly related to the current poor popularity of the Internet content rating system. I will discuss this issue in depth further on (see Chapter 5.5).

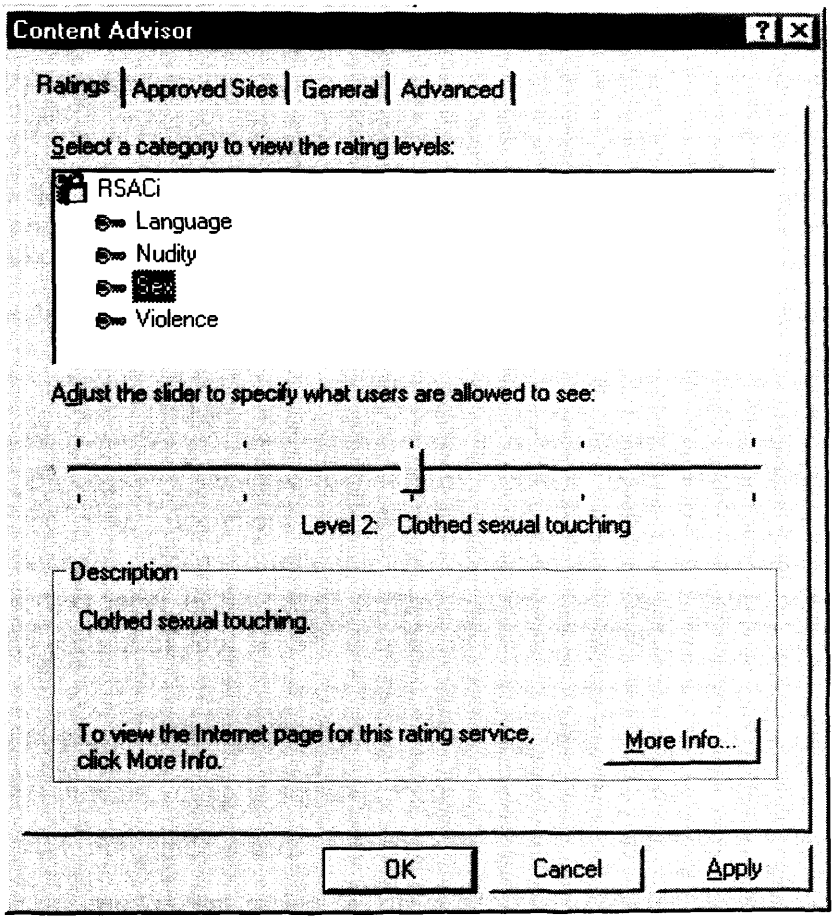

Fig. 5.1. Microsoft IE Content Advisor with the RSACi system

However, this kind of standardisation and categorisation can be problematic, since contextual factors of vocabulary elements are easily excluded in those processes. Vocabulary elements may reflect a certain community's moral and

cultural values, although information available on the Internet holds very diverse viewpoints. For these reasons, W3C has encouraged the development of a wide range of rating systems in order to maximise user choice. Since PICS allows Internet users to "have easy access to the widest possible range of content selection products, and a diversity of voluntary rating systems" (W3C, 1998), any PICS-compliant software can process any PICS-compliant labels which are provided by various entities. In principle, users can choose their rating services and software, according to their different cultural, political, and religious viewpoints.

Secondly, in order to rate a Website, certain labels should be assigned to the site. Rating can be done not only by the site creator, referred to as the first-party, but also by a third-party. A typical procedure of first-party labelling is as follows:

> [...] you choose a self-labelling service, connect to its Web server and describe your document or Website by filling out an on-line questionnaire. After completing the questionnaire, the service gives you a text label in a special format, which you then paste into the header portion of your HTML document (W3C, 2000b).

Unlike first-party labelling, third-party labelling runs through a server, the so-called label bureau, which is separate from a Web document. This server is "an HTTP server that understands a particular query syntax" and "can provide labels for documents that reside on other servers." (Miller, 1996) Third-party labelling can be done without any acknowledgment of site creators or information providers.

Thirdly, labels should be transmitted to Internet users who request them for filtering. For transmitting labels, first-party and third-party labelling use

different methods. In first-party labelling, according to a user's request, one or more labels which are embedded in the header of a Web document are fetched by a browser or stand-alone filtering software. A PICS label places at the head of a HTML document, the <head> section which usually carries metadata of the document. The following is an example of embedding a PICS label in an HTML document:

```
<html>
  <head>
    <title>PICS Label Example</title>
    <META http-equiv="pics-label" content='(pics-1.1
    "http://www.rsac.org/ratingsv01.html" l gen true
    for "http://www.btinternet.com/~yskim" r (n 0 s 0 v 0 l 0))'>
  </head>
  <body>
.....
```

According to W3C (2000b), in third-party labelling, labels are transmitted through label bureaus.

> When an end-user asks to see a particular URL, [...] a software filter makes an inquiry to the label bureau to ask for labels that describe that URL. Depending on what the labels say, the filter may block access to that URL.

Resnick and Miller (1996) describe third-party labelling as follows:

> The third way to distribute labels is through a label bureau that dispenses only labels. A bureau can distribute labels created by one or more services. This separation of labels from content allows third-party labelling even when the publishers do not wish to distribute the labels. [...] A label bureau is implemented as an HTTP server that accepts URL query strings in a special format.

The procedure is illustrated below (Fig. 5.2).

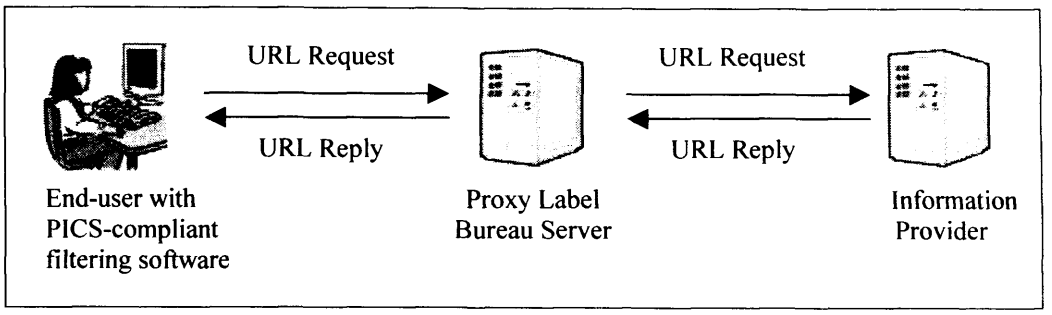

Fig. 5.2. Third-party labelling

A sample request made to a label bureau may be as follows (Resnick & Miller, 1996):

```
GET /Ratings?opt=generic&
        u="http%3A%2F%2Fwww.questionable.org%2F"&
        s="http%3A%2F%2Fwww.rating.org%2Fv2.5"
        HTTP/1.0
```

This query requires a label bureau to send a single label for the Website (http://www.questionable.org). The rating service (http://www.rating.org/v2.5) should have created a desired label. A URL query string is necessary to encode ":" as "%3A" and "/" as "%2F", since Unicode is the internal character set for PICSRules rules.

Fourthly, the development of PICS-compliant filtering software is needed. As discussed above, since PICS is a technical standard, it cannot operate without filtering software which deals with PICS labels. Currently the most common type of label filtering software is a Web browser such as Microsoft Internet Explorer. There are many types of stand-alone filtering software, including Cyber Patrol, and CYBERsitter, which support PICS-based rating as mentioned in Chapter 4.

Fifthly, users who want to use PICS-based rating systems should choose a

rating service which can associate with filtering software. Finally, installing and running PICS-compliant filtering software are the last steps. The software can take place not only at end-user level, but also upstream such as a proxy server, a search engine and an Internet service provider. Since PICS allows the possibility of upstream filtering many Internet libertarian organisations, such as the Global Internet Liberty Campaign (GILC, 1997), have criticised PICS for threatening end-users' autonomy and rights to freedom of expression. This issue will be discussed in detail later in this chapter.

5.2.2. PICSRules

While, as mentioned above, PICS is merely a technical standard which is related to labelling and distributing of metadata, PICSRules is associated with the practical implementation of rating systems. W3C defines PICSRules as "a language for writing profiles, which are filtering rules that allow or block access to URLs based on PICS labels that describe those URLs." (W3C, 1997b) The most significant ability of PICSRules is that it is able to coordinate various rating systems through multiple policy clauses.

> [A] PICSRules rule can specify one or more PICS rating services to use, one or more PICS label bureaus to query for labels, and criteria about the contents of labels that would be sufficient to make an accept or reject decision (W3C, 1997b).

Using PICSRules' policy clauses, access to a specific set of URLs can be blocked or allowed based on PICS labels. Here is an example:[9]

---

[9] The URL, *http://www.example.org* is not a real domain name. It is used only for this example. It is reserved for use in documentation by the Internet Society and is not available for registration.

```
(PicsRule-1.1
        (
        serviceinfo (
            "http://www.example.org/ratings/v01.html"
            shortname "Ex"
            bureauURL
"http://labelbureau.example.org/ratings"
            UseEmbedded "N"
            )
        Policy (RejectIf "(Ex.Nudity > 3)")
        Policy (AcceptIf "otherwise")
      )
)
```

This example means that access to certain URLs is prohibited by a rating service. Each clause of the rule purports as follows (Table 5.2):

Serviceinfo clauses	
"http://www.example.org/ratings/v01.html"	A rating service URL
shortname "Ex"	—
bureauURL "http://labelbureau.example.org/ratings"	A label bureau URL
UseEmbedded "N"	Ignoring labels embedded in the Web document
Policy Clauses	
Policy (RejectIf "(Ex.Nudity > 3)")	Documents which are labelled higher than level 3 on the "Nudity" scale of the "Ex"
Policy (AcceptIf "otherwise")	Access to everything else will be allowed, including unlabelled documents

Table 5.2. PICSRules clauses

Even without using any PICS labels PICSRules can filter a specific set of URLs. The following example of PICSRules forbids access to any URLs that are hosted under *www.example.com* or *www.example.net*,[10] while any other

[10] The URLs *http://www.example.com* and *http://www.example.net* are not real domain names. These domain names are used only for this example. Just like *http://www.example.org*, these two

URLs are allowed access:

```
(PicsRule-1.1
        (
        Policy (RejectByURL ("http://*@www.example.com:*/*"
                             "http://*@www.example.net:*/*"))
        Policy (AcceptIf "otherwise")
        )
 )
```

5.2.3. RDF

The Resource Description Framework, developed by W3C, is another foundation for supporting metadata. It provides common structures that can be used for the Extensible Markup Language (XML) data exchange (W3C, 2001). It is applicable in a variety of areas:

> [...] in *resource discovery* to provide better search engine capabilities, in *cataloging* for describing the content and content relationships available at a particular Website, page, or digital library, by *intelligent software agents* to facilitate knowledge sharing and exchange, in *content rating*, in describing *collections of pages* that represent a single logical "document", for describing *intellectual property rights* of Web pages, and for expressing the *privacy preferences* of a user as well as the *privacy policies* of a Website. RDF with *digital signatures* will be key to building the "Web of Trust" for electronic commerce, collaboration, and other applications (W3C, 1999).

However, for the purpose of this study the discussion will be limited to issues relating to content rating.

The basic RDF model consists of three object types: resources, properties and

---

domain names are reserved for use in documentation by the Internet Society and are not available for registration.

statements. Firstly, *resources* means all things described by RDF expressions, such as an entire Website, a part of a Web page, and even an object that is not directly accessible via the Web. Secondly, a *property* is a specific aspect, characteristic, attribute, or relation used to describe a resource. Thirdly, a *statement* is a specific resource together with a named property plus the value of that property for that resource. A statement contains these three elements which are called *subject*, *predicate*, and *object* respectively (W3C, 1999). Just as a PICS label contains several different ratings, a single RDF statement is able to assign a number of properties. Here is an example:

> A description of worldwarII.com/dday/omaha.jpeg might consist of a single *statement* attributing four *properties* here, "picture," "real-life," "historical," and "violence." For the properties "picture," "real-life," and "historical" the scale would probably have only the values 1 and 0, corresponding to "Yes" and "No." The property "violence" might have a broader range of values—it might, for example, be the RSACi Violence category, in which case its scalar values would range from 0 to 4, and worldwarII.com/dday/omaha.jpeg would receive a 3 (Balkin, Noveck & Roosevelt, 2000, p. 228).

Indeed, RDF is quite similar to PICS. It can express anything that PICS can. Furthermore, it provides "a model for representing metadata that is even more general than PICS with more express power." (W3C, 2000c) RDF has a class system. A collection of classes is called a schema. A PICS rating service description is analogous to an RDF schema. In this sense, RDF is referred to as a successor to PICS. The Information Society Project group at Yale Law School predicts, "some form of RDF-based system will eventually supersede PICS-based filtering." (Balkin, Noveck & Roosevelt, 2000, p. 229) Phil Archer (2004), chief technology officer of ICRA, stated;

> As an XML-based technology, RDF can be deployed just as easily in mobile communications infrastructure as on the fixed Internet, as well as any other medium that has occasional or permanent network access such as games consoles and digital TV. The potential is significant.

In my view, however, it is too early to make any assumptions regarding RDF-based filtering, because it has been just a few years since its predecessor, PICS-based filtering, constituted the standard of Internet content rating. However, not every function of PICS and PICSRules has yet been used. For instance, PICSRules' multi-policy clauses are hardly applied to rating systems, although they have the potential to coordinate various rating systems.

In February 2003, ICRA launched a new project which is named "Customisation and Personalisation thorugh RDF." According to ICRA (2003a), the project aims at developing "a truly cross-media platform, usable in all types of network devices and many types of consumer electronics, such as DVD and MP3 players, through which multiple classification systems may be expressed along with other metadata." Once ICRA announced that new labelling and filtering tools which use RDF would be made available to demonstration standard in late 2003, but it did not happen. ICRA is still working on this project to date in May 2004.

5.3. Internet Content Rating System: Technical Analysis

Now, I will explore three Internet content rating systems; the SafeSurf system, the RSACi system and the ICRA system, mainly from technical aspects. Both the SafeSurf system and the RSACi system are two of the earliest practical PICS-based rating systems which were developed in 1995 and early 1996 respectively. They were almost simultaneously developed with PICS. Before the advent of the ICRA system, the RSACi system was the most widespread

system worldwide. While these two systems are based in the US, the ICRA system is developed under the European Commission's 'Action Plan for Promoting Safer Use of the Internet.'

5.3.1. The SafeSurf System

The SafeSurf system is one of the early-developed, well-known Internet content rating systems which is based in the US. It was developed by Ray Soular and Wendy Simpson in 1995. The SafeSurf system rates Web content on a scale of one to nine in ten categories. The categories include *age, profanity, heterosexual themes, homosexual themes, nudity, violence, intolerance,*[11] *glorifying drug use, other adult themes* and *gambling.* All categories are given a numeric order according to level. The mildest level is number one and the most severe level is nine. The level value cannot be zero because this means the classification has no level or does not exist (Soular & Simpson, 1995). The full text of the "SafeSurf SS~~ Rating Standard" is in Appendix D.

The SafeSurf identification standard is recognised by the certification mark, SS~~, which is referred to as the SafeSurf Wave, followed by three digits, one space and a numeric value. The classification types ranging from zero to nine then A to Z are identified by three digits. The last numeric value identifies the level. An example of the SafeSurf rating system in a Web document is as follows:

```
<META http-equiv="PICS-Label" content='(PICS-1.1
"http://www.classify.org/safesurf/"
l gen true for "http://www.btinternet.com/~yskim/" r (SS~~000 1))'>
```

[11] Intolerance of another person's racial, religious, or gender background.

This meta tag is for my own personal Website. It means that my site does not contain any theme of the SafeSurf's nine categories. This meta tag is generated by the SafeSurf Rating Form. This kind of meta tag generation form has been also adopted by other rating systems, such as the RSACi system and the ICRA system. The World Wide Web Consortium describes it as follows:

> [It] is a fully-automated, paperless system that relies on a quick, easy-to-use questionnaire that the Webmaster completes at [a rating service Website]. The questionnaire runs through a series of highly specific questions about the level, nature and intensity of [each category] found within the Webmaster's site. Once completed, the questionnaire is then submitted electronically to [a rating service's] Web Server, which tabulates the results and produces the HTML advisory tags that the Web master then places on their Website/page (W3C, 1996).

If a site contains several adult themes, the syntax of the label may be as follows:

```
<META http-equiv="PICS-Label" content='(PICS-1.1
"http://www.classify.org/safesurf/" l gen true for "http://www.example.com"
r (SS~~000 6 SS~~001 1 SS~~002 2 SS~~003 6 SS~~004 7 SS~~005 8
SS~~007 9 SS~~008 2 SS~~009 3 SS~~00A 4))'>
```

This syntax means the Website is for adults and contains profanity with a level of 1, heterosexual theme with a level of 2, homosexual theme with a level of 6, nudity with a level of 7, violence with a level of 8, intolerance with a level of 9, glorifying drug use with a level of 2, other adult themes with a level of 3 and gambling with a level of 4. Each level of this sample is described as follows (Table 5.3):

Syntax	Category	L*	Description
SS~~000 6	Age Range	6	Adults
SS~~001 1	Profanity	1	Subtle Innuendo: Subtly Implied through the use of Slang
SS~~002 2	Heterosexual Themes	2	Explicit Innuendo : Explicitly implied (not described) through the use of metaphor
SS~~003 6	Homosexual Themes	6	Graphic : Descriptions of intimate sexual acts
SS~~004 7	Nudity	7	Detailed Graphic : Erotic frontal nudity
SS~~005 8	Violence	8	Inviting Participation in Graphic Interactive Format
SS~~007 9	Intolerance	9	Advocating Violent or Hateful Action
SS~~008 2	Glorifying Drug Use	2	Explicit Innuendo
SS~~009 3	Other Adult Themes	3	Technical Reference
SS~~00A 4	Gambling	4	Non-Graphic-Artistic, Advertising

Table 5.3. Description of the sample label * **L**: Level

5.3.2. The RSACi System

The RSACi system was developed by the Recreational Software Advisory Council (RSAC) which is an independent, non-profit organisation based in the US. RSAC was established in 1994 to rate video games for violent content, bad language, sex and nudity. "The original RSAC rating system was developed in September 1994 in direct response to the threat of congressional legislation that sought to control levels of violence in the computer game market." (W3C, 1996) Since then, RSAC has extended its original rating system to the Internet largely in response to the attempts of the US government to regulate indecent information on the Internet. RSACi is an acronym for the Recreational Software Advisory Council on the Internet. In this sense, it can be said that the RSACi system is an offshoot of the former RSAC system. In November 1995 the RSACi Working Group had its first meeting with representatives from Microsoft, ATT, Bell Atlantic, Time Warner and others. In February 1996 RSAC announced the launch of RSACi and since April 1996 the RSACi rating

system has been available to the public.

The RSACi system rates Web content in four categories: violence, nudity, sex, and language on a scale of 0 to 4, from "None" through progressively stronger examples (Table 5.4).

	Violence Rating Descriptor	Nudity Rating Descriptor	Sex Rating Descriptor	Language Rating Descriptor
LEVEL 4	Rape or Wanton, Gratuitous violence	Frontal nudity (qualify as provocative display)	Explicit sexual acts or sex crimes	Crude, vulgar Language or extreme Hate speech
LEVEL 3	Aggressive violence or death to human	Frontal nudity	Non-explicit sexual acts	Strong language or hate speech
LEVEL 2	Destruction of realistic objects	Partial nudity	Clothed sexual touching	Moderate expletives or profanity
LEVEL 1	Injury to human being	Revealing attire	Passionate kissing	Mild expletives
LEVEL 0	None of the above or sport related	None of the above	None of the above or innocent kissing; romance	None of the above

Table 5.4. RSACi rating system descriptors (Retrieved March 11, 2000, http://www.icra.org/about.html)

RSACi is currently governed by the Internet Content Rating Association (ICRA), since RSAC transferred its assets, including the RSACi system, to ICRA in April 1999. Thus, RSAC not longer exists. However, it does not necessarily mean that the RSACi system is not working any more. The latest version of Microsoft Internet Explorer (version 6.0) still has the RSACi system as its default rating system. It is the only rating system which Microsoft IE has adopted as a default option. For this reason, it is still one of the most widespread Internet content rating systems worldwide. The RSACi label is now provided by ICRA alongside the ICRA label. For instance, CNet.com has

both labels as follows:

```
<meta http-equiv="pics-label" content='(pics-1.1
"http://www.icra.org/ratingsv02.html" l gen true for
"http://www.cnet.com" r (cz 1 lz 1 nz 1 oz 1 vz 1)
"http://www.rsac.org/ratingsv01.html" l gen true
for "http://www.cnet.com" r (n 0 s 0 v 0 l 0))' />
```

Although it has had this advantage, its popularity is rather disappointing. According to a report, by October 2000 about 150,000 Websites have rated themselves with the RSACi system (Keller & Verhulst, 2000). ICRA states that those rated Websites includes a great proportion of the top 100 sites which account for 80 percent of the whole traffic on the World Wide Web (ICRA, 1999). Stephen Balkam, executive director of ICRA, also said "those who have rated include many of the most heavily trafficked Websites." (Mendels, 1999) However, this number is very small compared to the number of total Web pages on the Internet. According to a report from Cyveillance, by July 2000, the total number of pages on the Internet already surpassed 2.1 billion, and more than 7 million new pages are being added each day (Cyveillance, 2000). On 26th July 2000 I examined the top 19 sites to find whether they use the rating system and the results disappointed me. I selected 19 Websites based on "The Web's 100 most popular sites." (http://www.100hot.com) Of these, only five sites were rated by the RSACi system. The second test was conducted on 12th February 2002. The result of the second test was almost the same as the first test, except that four sites which were already rated by the RSACi system had newly adopted the ICRA system. I conducted the third test on 4th June 2003. Seven out of 19 sites label their sites using the RSACi system or the ICRA system. The results are as follows (Table 5.5):

	Site	URL	Rating		
			July 2000	Feb. 2002	June 2003
1	Yahoo	http://www.yahoo.com	R*	R/I**	R / I
2	Microsoft Corp.	http://www.microsoft.com	R	R	R
3	MSN	http://www.msn.com	R	R / I	R / I
4	RealNetworks	http://www.real.com			
5	Lycos	http://www.lycos.com			
6	AOL	http://www.aol.com	R	R / I	R / I
7	Netscape	http://home.netscape.com			R
8	Altavista	http://www.altavista.com			
9	Spedia	http://www.spedia.com			
10	Excite	http://www.excite.com			
11	WebCrawler	http://www.webcrawler.com			R
12	Go.com	http://www.go.com			
13	CNET	http://www.cnet.com	R	R / I	R / I
14	USANET	http://www.usa.net			
15	Homestead.com	http://www.homestead.com			
16	CNN	http://www.cnn.com			
17	Snowball.com	http://www.snowball.com			
18	Amazon.com	http://www.amazon.com			
19	Google	http://www.google.com			

Table 5.5. Usage of the RSACi and the ICRA systems among the top 19 sites * **R**: The RSACi system ** **I**: The ICRA system

As presented in the above table (Table 5.5), during the last three years there is no significant change in the number of rated Websites. This kind of poor popularity does not affect only the RSACi system. All the PICS-based Internet content rating systems which are currently available have suffered from the same problem. Since many of the above 19 sites are portals, search engines and news sites which contain a vast amount of varied information, it may not be easy to rate themselves by a single category. However, it does not mean that there is no need to rate these sites. The number of rated Websites is vital,

because the success of the rating system largely depends on it. The rating system needs to reach a critical mass for achieving its practical force. For this reason, ratings of these heavily trafficked, popular and influential sites are important. I will discuss this issue later in this chapter (see Chapter 5.5).

Although both the SafeSurf and RSACi rating systems are based on PICS, the two rating systems are slightly different. First of all, as compared to the RSACi system, the SafeSurf rating system gives attention to contextual factors of vocabulary elements. For instance, nudity can be presented not only in an adult magazine but also in a medical textbook or science magazine, simply measuring the degree of nudity is not enough. Hence, the SafeSurf system includes 'technical reference,' 'non-graphic-artistic,' 'graphic-artistic' and 'graphic' as vocabulary elements for its categories. Despite the difference between them, however, "both have drawn some complaints of American cultural bias." (Keller & Verhulst, 2000) Therefore, many institutions in Europe, such as INCORE, INHOPE and the European Commission, have made efforts to establish Internet content rating systems for the European and International markets. As a result, in December 2000 ICRA introduced the new ICRA labelling system.

5.3.3. The ICRA System

In March 1999 ICRA incorporated as a non-profit organisation in London and was officially launched two month later. It has offices in the UK in Brighton and in the US in Washington, D.C. ICRA has received project funding from the European Commission under the 'Action Plan for Promoting Safer Use of the Internet' and is supported by many non-profit organisations and Internet

companies.[12] Unlike other rating systems, such as SafeSurf and RSACi, the ICRA system is a multi-party rating system (MPRS) that is theoretically based on the layer cake model which was proposed by the Information Society Project at Yale Law School. The layer cake model can be illustrated as follows (Fig. 5.3):

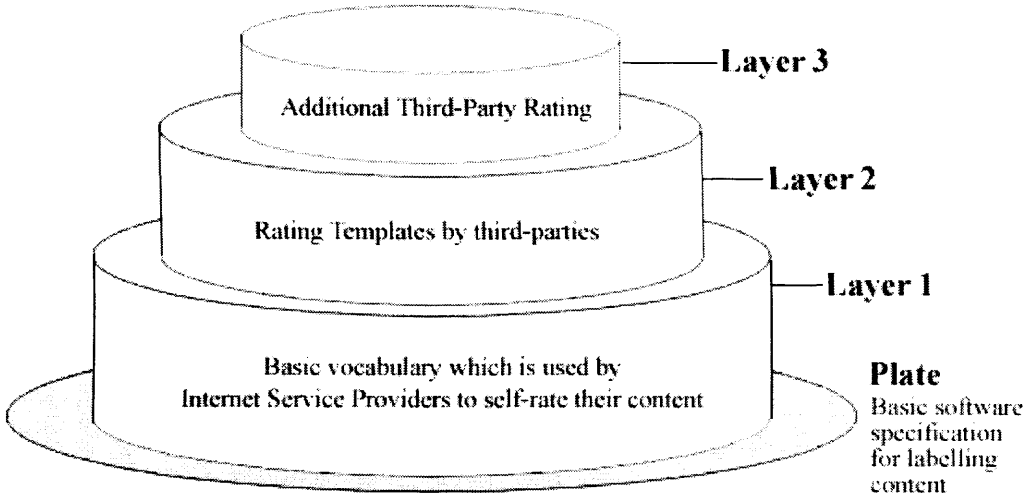

Fig. 5.3. Layer cake model (Balkin, Noveck & Roosevelt, 2000; Keller & Verhulst, 2000)

The plate is the software specification which includes PICS, PICSRules and RDF. The first layer of the cake is a basic vocabulary that is used by first-parties in rating their sites. In the ICRA system first-parties do not rate their Web content sites in certain categories on scalar numbers of levels. Instead, they list all vocabulary elements which are applicable to their Web content. In other words, the ICRA system separates the vocabulary elements from the construction of rating templates. In my view, this feature makes the system relatively objective and value-neutral as compared to other rating systems,

[12] The members of ICRA include AOL Europe, Bell Canada, British Telecom, Cable & Wireless, Digimarc, IA Japan, Microsoft, Parents Advisory Group for the internet, R3Net, SIIA, T-Online, Tiscali, Verisign, Verizon and Yahoo! (Resource: ICRA website. Retrieved June 5, 2003, from *http://www.icra.org*)

since the construction of rating templates inevitably involves some degree of value-judgment. This procedure can be described as follows:

> [First-parties] fill out a questionnaire with simple descriptive information [...] ICRA converts this information into a label expressing the descriptive information in machine-readable PICS format and [the first-parties] put the labels into the source code for their Webpage (Keller & Verhulst, 2000).

The ICRA system has 45 descriptors. Up to 40 descriptors can be selected together. As of March 2004, its labelling questionnaires and filtering interfaces are available in several languages, including English, German, French, Spanish and Chinese (Hong Kong). The ICRA descriptors and codes are as follows (Table 5.6):

	Descriptor	ICRA Code	RSACi Code
Chat	Chat	ca	
	Moderated chat suitable for children and teens	cb	
	None of the above	cz	
Language	Explicit sexual language	la	l4
	Crude words or profanity	lb	l2
	Mild expletives	lc	l1
	None of the above	lz	l0
Nudity & Sexual Material	Erections or female genitals in detail	na	n4
	Male genitals	nb	n3
	Female genitals	nc	n3
	Female breasts	nd	n2
	Bare buttocks	ne	n2
	Explicit sexual acts	nf	s4
	Obscured or implied sexual acts	ng	s3
	Visible sexual touching	nh	s3
	Passionate kissing	ni	s1
	None of the above	nz	s0
	Context - Artistic	nr	–
	Context - Educational	ns	–
	Context – Medical	nt	–
Other Topics	Promotion of tobacco use	oa	
	Promotion of alcohol use	ob	
	Promotion of drug use	oc	
	Gambling	od	
	Promotion of weapon use	oe	
	Promotion of harm against people	of	
	Material that might be perceived as setting a bad example for young children	og	
	Material that might disturb young children	oh	
	None of the above	oz	
Violence	Sexual violence / rape	va	v4
	Blood and gore, human beings	vb	v4
	Blood and gore, animals	vc	v4
	Blood and gore, fantasy characters (including animation)	vd	v4
	Killing of human beings	ve	v3
	Killing of animals	vf	v3
	Killing of fantasy characters (including animation)	vg	v3
	Deliberate injury to human beings	vh	v1
	Deliberate injury to animals	vi	v1
	Deliberate injury to fantasy characters (including animations)	vj	v1
	Deliberate damage to objects	vk	v1
	None of the above	vz	v0
	Context - Artistic	vr	–
	Context - Educational	vs	–
	Context – Medical	vt	–
	Context - Sports	vu	–

Table 5.6. The ICRA descriptors and associated codes

Here is an example of the ICRA label. ICRA provides the RSACi label alongside its new label:

```
<meta http-equiv="pics-label" content='(pics-1.1
"http://www.icra.org/ratingsv02.html" comment "ICRAonline EN v2.0" l
gen true for "http://www.example.com" r (nh 1 ni 1 vz 0 vr 1 lc 1 oa 1 ob 1
ca 1) "http://www.rsac.org/ratingsv01.html" l gen true for
"http://www.example.com" r (n 0 s 3 v 0 l 1))'>
```

In this label, each ICRA code means as follows (Table 5.7):

ICRA Code	Explanation
nh 1	Visible sexual touching is present on the site.
ni 1	Passionate kissing is present on the site.
vz 0	None of the violence materials, which are listed in the table of the ICRA descriptors, is present on the site, but a violence material may appear in an artistic context or in an educational context or in a medical context and is suitable for young children or in a sports related context.
vr 1	A violence material appears in an artistic context and is suitable for young children.
lc 1	Mild expletives are present on the site.
oa 1	The site promotes tobacco use.
ob 1	The site promotes alcohol use
ca 1	The site offers Unmoderated chat

Table 5.7. The ICRA codes of the sample label

The second layer consists of rating templates which are created by third-parties. Third-parties take certain vocabulary elements and arrange them into categories and scalar orders. Thus, third-parties do not have to rate enormous numbers of Websites in order to create templates. The cost of creating templates can therefore be significantly reduced. In this sense, it is expected that each third-party may provide different templates that reflect diversity of information on the Internet. An expert report from the Information Society

Project states that:

> [By] combining a basic vocabulary at level one with flexibility at level two we can achieve much greater diversity and provide more end-user choice than in a unitary system (Balkin, Noveck & Roosevelt, 2000, p.247).

The third layer is a set of third-party ratings of individual sites. For instance, any URL-based filtering systems which are compatible with PICS can be placed at the third layer. However, as discussed in the previous chapter, URL-based filtering has a number of serious drawbacks concerning end-users' autonomy and free speech rights, although it is one of the most popular technical solutions. But it is feared that there is a possibility that this kind of additional third-party rating can have a negative effect on the rest of the layer structures. As discussed in the previous chapter, the so-called first generation filtering technologies pose serious technical shortcomings and have been criticised for violating end-users' autonomy (see Chapter 4.4).

For better implementation of the ICRA label system, ICRA launched its stand-alone software, ICRA*filter*, in March 2001. This stand-alone software which is free supports blacklist based filtering and third-party templates (Fig. 5.4). As of March 2004, Anti-Defamation League and Kidstation.de provide their own templates for the ICRA*filter*. These templates are downloadable from their Websites; *www.adl.org* and *www.kidstation.de* for free. However, these templates do not provide end-users with detailed information about what sites would be blocked or allowed by them. Their URL lists are encrypted. This feature may raise contentions concerning end-users' autonomy and freedom of expression.

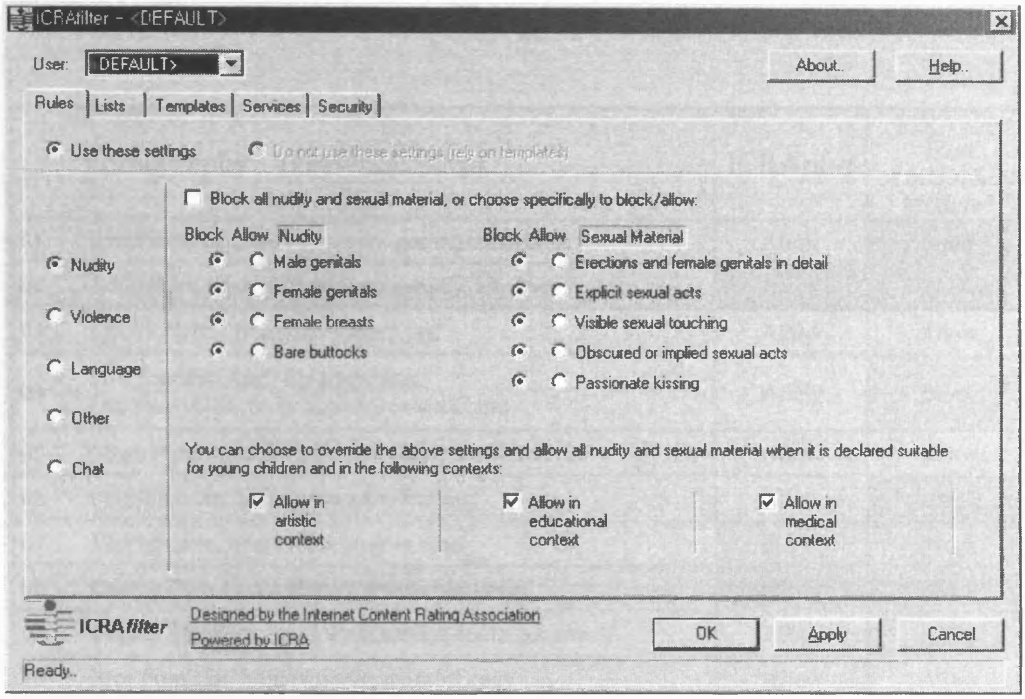

Fig. 5.4. The ICRA*filter*

Almost three years after the ICRA*filter* was launched, the ICRA released its latest software, ICRA*plus*, in November 2003. It employs additional controversial technologies, such as content analysis by artificial intelligence agents and image recognition technologies (ICRA, 2003b). As discussed in Chapter 4, these kinds of filtering technologies are rarely applied to commercial filtering software, because of their technical imperfections. ICRA*plus* allows users to add third-party filter modules. Users can choose multiple filter modules at the same time. According to the ICRA, "ICRA*plus* is more than just another Internet filter. It is the foundation that allows you to select and combine several filters" Currently, two filter modules, one is free and another one is commercial, are available via the ICRA Website. The commercial filter's annual subscription fee is 35 EUR. In order to examine the filtering effectiveness of ICRA*plus*, In May 2004 I tested it against a set of 20 Websites which were generated to test the first generation filtering software in

Chapter 3. The result is as follows (Table 5.8):

	Pornography (keyword: porn)	ICRA*plus*	ICRA*plus* *With A additional Module**
01	PornResource.com, http://www.pornresource.com/	Allow	**Block**
02	Adult Sites Against Child Pornography, http://www.asacp.org/	**Block**	**Block**
03	LEGO PORN, http://www.asacp.org/	Allow	Allow
04	Free Extreme Adult Entertainment, http://www.cybererotica.com/free-sites.html	Allow	**Block**
05	Mega Porn Links, http://www.mega-porn-links.com/	Allow	Allow
06	Porn-Free.org, http://www.porn-free.org/	Allow	**Block**
07	MyPorn.com, http://www.myporn.com/	**Block**	**Block**
08	Quality Porn Links, http://www.penisbot.com/	**Block**	**Block**
09	Here Is The Porn, http://www.hereistheporn.com/main/	Allow	**Block**
10	Free Porn List, http://www.freepornlist.com/	Allow	Allow
11	Porn-Station, http://www.porn-station.com/Directory/New/	Allow	Allow
12	Porn Passwords, http://www.porn-passwords.net/	Allow	**Block**
13	Asian Spreads, http://www.japanese-porn.org/	Missing	Missing
14	Hosts for Porn, http://hosts4porn.com/	Allow	**Block**
15	XXX Asian Porn Pics, http://www.xxxasianporn.net/	Allow	**Block**
16	Free Daily Pics, http://www.karasxxx.com/potd/newmainpotd.shtml?tekiegeek:pd	Allow	**Block**
17	Report Child Porn to Government Agencies, http://www.reportchildporn.com/	Allow	**Block**
18	TokyoPorn.com, http://www.tokyoporn.com/	Allow	**Block**
19	Legal Porn, http://www.legalporn.com/	Allow	Allow
20	We Love Free Porn, http://www.welovefreeporn.com/	**Block**	**Block**

Table 5.8. ICRA*plus* filtering test * Jugendschutzprogramm.de

In this test ICRA*plus* omits a number of pornography Websites, while it blocks an anti child pornography campaign Website (http://www.asacp.org). Only three pornography sites are filtered out by ICRA*plus*. However, when an additional filter module, Jugendschutzprogramm.de, is added to ICRA*plus*, the filtering results significantly enhance. With the additional module ICRA*plus*

blocks 14 sites out of the 20 sample sites. However, it still omits four hard-core pornography sites, such as Mega-Porn Links, Free Porn List, Porn-Station and Legal Porn. Just like many other commercial filtering software, it also has over and under-blocking problems.

In sum, the ICRA system is a more flexible and relatively objective solution compared to other rating systems. Furthermore, it provides globally translatable descriptors. However, this does not mean that the ICRA system is a perfect solution. It still has many problems as do RSACi and SafeSurf. Another concern is that its stand-alone filtering software increasingly emphasises the first generation filtering methods rather than its original labelling system, thus it resembles other commercial filtering software. In the next section the advantages and disadvantages of those Internet content rating systems will be critically discussed.

5.4. Advantages of the Internet Content Rating System

The rating systems which are based on the PICS specifications are more sophisticated compared to first generation filtering software. While first generation filtering software manually rates individual Web pages only as "adult or child safe", or "block or no-block", the PICS-based rating software rates Web pages along multiple dimensions such as violence, nudity, sex, and language. They also allow users to control any number of values for any given dimensions. For instance, a parent can block only sites rated over 3 for violence and 8 for sex. This means that parents are able to create their own filtering rules for their children. It means that the PICS-based rating software can be customised by any end-user. This flexibility is a very important feature as far as end-users' autonomy is concerned, since not everyone necessarily wants to block the same Web pages. In my view, the PICS-based rating system

is a significant advance in Internet filtering software. The theory of PICS empowers Internet users to control their own access to Internet content, and would reduce the risk of government censorship. Despite these advanced features, Internet content rating systems have been criticised for many reasons, from technical issues to issues of free speech.

5.5. Technical Disadvantages of the Internet Content Rating System

As regards technical issues, the first point of critique is that there is an easy loophole to circumvent the rating system. While Microsoft IE version 4 or above has supported various PICS-based rating systems through its Content Advisor, the Netscape Communicator version 4.7x assisted only two PICS-compliant rating systems, RSACi and SafeSurf, through its built-in ratings protection feature, NetWatch. However, its latest version 7.0 does not provide any rating systems. Furthermore, other popular browsers, Opera and Mozilla Firefox, do not support any rating system. Using these Web browsers, children can easily evade the system. This issue appears to be getting serious, since Firefox has continued to steal market share from Microsoft IE — as of January 2005, while use of Firefox rose to over six percent, Microsoft IE's market share dropped to below 90 percent (Claburn, 2005).

The second point of critique is that the Internet content rating system's filtering coverage is very narrow. The system is currently working only on the World Wide Web, while first generation filtering software is generally able to filter most types of Internet communications. According to statistics from the IWF covering the last six years, Usenet is a significantly problematic part of the entire Internet (see Chapter 4.3.1). It cannot be rated by the PICS system. E-mail, chat room, FTP and newsgroup are also beyond the PICS-based rating's targets. In my view, rating e-mail or chat rooms poses serious problems as

regards the right to privacy. There are tens of thousands of chat rooms on the Internet. Millions of people worldwide send and receive e-mails and news from their friends, newsgroups and mailing lists every day. Nobody wants to rate personal post or telephone calls, but some people want to do this on the Internet.

The third point of critique of the Internet content rating system is about whether or not the system can be enforced. The success of the Internet content rating system, including the ICRA system, largely depends on the number of rated Websites. In order to achieve a viable rating system, it should reach a critical mass. However, currently the number of rated Websites constitutes too small a proportion of the total number of Websites, though ICRA has made great efforts to promote its rating system with the European Commission's support. Keller and Verhulst (2000) explain through their report, *Parental Control in a Converged Communications Environment: Self-Regulation, Technical Devices and Meta-Information*, the following:

> Since the ICRA model relies largely on uncompensated effort by both first-party content providers and third-party list makers, it is important to find means to both encourage participation as easy as possible.

However, so far, no Internet content rating system seems to find that means. Poor participation results in poor enforcement of the rating system, and then this poor enforcement reproduces people's poor involvement on an enlarged scale. In this context the South Korean government attempts to mandate the Internet content rating system, despite severe criticism of censorship – I will discuss this issue in Chapter 7 in depth. In my view, the best solution to gain the public's popularity is providing a rating system which is easily accessible and user-friendly. In this context the rating system would be loaded into Microsoft IE as a default top menu. Developing stand-alone software which is

similar to many other commercial filtering products cannot be the right answer. At least the ICRA system would have been a default rating system of Microsoft IE. Nevertheless, it is not expected that the ICRA system becomes its default rating system, since the European Union has prevented the US-based company from being an official partner of its 'Action Plan for Promoting Safer Use of the Internet.' According to Phil Archer (2004);

> An initial aim for ICRA was that Microsoft would update the Content Advisor function in Internet Explorer to read ICRA labels rather than the old RSACi System. Indeed, Microsoft was to be a partner in the original project. That proved to be impossible, however, as EU rules prevented the US-based software company from being an official project partner. By early 2001 it had became clear that ICRA would need to offer an alternative label-reading system. The result was ICRA*filter*, a tool that demonstrated the concept of filtering against ICRA labels.

5.6. The Right to Free Speech and the Internet Content Rating System

Apart from the technical defects of the Internet content rating system, many libertarians and civil organisations, such as the ACLU and the Global Internet Liberty Campaign (GILC), have argued that the PICS-based rating system may violate freedom of expression on the Internet. Cyber-Rights & Cyber-Liberties (UK) (1998) argues that third party rating systems do not guarantee transparency and accountability, and therefore may raise private censorship issues:

> [T]he use of third-party ratings systems pose free speech problems and with few third-party rating products currently available, the potential for arbitrary censorship increases [...]. This would mean that there will be no space for free speech arguments and dissent because the ratings will be done by private bodies and the governments will not be involved "directly." When censorship is implemented by government

> threat in the background, but run by private parties, legal action is nearly impossible, accountability difficult, and the system is not open or democratic.

The ACLU strongly objects to Internet content rating for reasons detailed in its report, *Fahrenheit 451.2:*[13] *Is cyberspace burning?* The ACLU insists that Internet content rating may cause controversial speech to be censored. Here is an example:

> Kiyoshi Kuromiya [14] of the Critical Path AIDS Project [www.critpath.org][15] has a website that includes safer sex information written in street language with explicit diagrams. He does not want to apply the rating "crude" or "explicit" to his speech, but if he does not, his site will be blocked as an unrated site. If he does rate, his speech will be lumped in with "pornography" and blocked from view. Under either choice, Kuromiya has been effectively blocked from reaching a large portion of his intended audience—teenage Internet users—as well as adults (ACLU, 1997).

Ironically, the same material can be distributed in print form in any bookstore without anyone worrying about having to rate it. Jonathan Wallace's article, *Why I will not rate my site* (Wallace, 1997b), gives another prime example. In 1995 he posted an article about the Holocaust, *An Auschwitz Alphabet* (Wallace, 1995), to the Web. Since then, in nine months, thousands people have visited his site, and hundreds of people have sent him e-mails to express thanks for making the site. Of course, some of them were minors. His concern started here. Under the existing rating system, the article may be rated as inappropriate

---

[13] "Fahrenheit 451" is a title of Ray Bradbury's novel which was initially published in 1953. The novel depicts the futuristic world where freedom of thought and speech are gone. Fahrenheit 451 is the temperature at which books burn.

[14] Kiyoshi Kuromiya, one of the world's leading AIDS activists, died on 10th May 2000, due to complications from AIDS.

[15] Retrieved June 6, 2003

information to a wide range of audiences, including teenagers, "because of several excerpts from the book, *The Nazi Doctors* (Lifton, 1986), describing castration and the removal of ovaries of camp inmates." He fears that rating systems may lump his article together with material containing obscene images of nude women.

In fact, the PICS-based rating systems have faced serious difficulties in dealing with contextual value, in just the same way as the first generation filtering software. The RSACi system excluded contextual factors from vocabulary elements. It could not distinguish between artistic nudity and obscene nudity (Balkin, Noveck & Roosevelt, 2000, pp. 251-254). Although the SafeSurf system provides wider and more detailed vocabulary elements for each category as compared to the RSACi system, it is not enough in my view to reflect the enormous diversity of information on the Internet. Indeed, the SafeSurf system has a serious problem with its vocabulary elements, since the terms which are used in its categories such as "artistic," "erotic" and "classic" may be interpreted as having different meanings depending on the cultural, religious, or political background. As previously mentioned, there are so many different standards relating to various aspects of life worldwide on the Internet that it is impossible to apply one subjective standard to the entire Internet community. Therefore, subjective rating categories are highly controversial. Objectivity is needed to retain reliability regarding rating systems.

In this sense, the ICRA system, which is referred to as the multi-party rating system, made an effort to provide potentially objective rating terminologies. It separates the vocabulary elements from the construction of rating templates which inevitably involves some degree of value judgment. Indeed, it has made a significant advance with regard to many aspects of the Internet content rating

system.[16] However, it does not yet provide a perfect solution. The ICRA system's descriptors do not provide absolute objectivity. In my view, its descriptors, such as "passionate kissing" and "material that might disturb young children" are rather subjective. Thus the ICRA system cannot be free from criticism against subjective value-judgment, just like other rating systems.

Furthermore, GILC even claims that the Internet content rating system empowers governments to control the access of their adult citizens. It argues that PICSRules can be used for the purposes of "enabling the development of country profiles to facilitate a global or universal rating system desired by governments," because it can block "access to content on entire domains, via the specification of full or partial domain names and/or IP addresses, regardless of the username, port number, or particular file path that is specified in the URL." (GILC, 1997) GILC asserts in its statement at the Internet content summit 1999 in Munich that: (GILC, 1999)

> First, the existence of a standardized rating system for Internet content [...] would allow governments to mandate the use of such a regime. By requiring compliance with an existing ratings system, a state could avoid the burdensome task of creating a new content classification system while defending the ratings protocol as voluntarily created and approved by private industry. [...] Second, the imposition of civil or criminal penalties for "mis-rating" Internet content is likely to follow any widespread deployment of a rating and blocking regime.

There is always a potential for people to cheat in their self-rating. For instance,

---

[16] According to the Final Report for the DVB Regulatory Group by Keller and Verhulst (2000), a multi-party rating system has a number of strengths as follows:

> [It] makes possible comparatively thorough coverage of the net. [It] enables individual parental control of content filtering [and] allows flexible adaptation across diverse cultural groups. [It also] draws on existing, globally applicable technological standards [and] operates with no direct cost to parents or content providers. [Furthermore, it] has the backing of major industry participants.

someone, who runs a commercial Website for adults realises that many people will not get to his or her site if it is either rated as "sexually explicit" or not rated at all. He or she may rate the Website "OK for minors." In addition, mis-rating can happen unintentionally because many Web pages contain much more complex information than the given rating categories can cope with. In this sense, the PICS-based rating systems which largely rely on the concept of self-rating may break down in the absence of a penalty system for mis-rating. The rating system may have the potential to lead to heavy-handed government censorship. Unfortunately, this nightmare has come true in South Korea. In Chapter 7, the Internet content rating system in South Korea, which has been strongly driven by the government, will be come under discussion.

5.7. Conclusion

Although the PICS-based rating system may be "an impressive second-best solution" (Weinberg, 1997), it is still not a satisfactory solution for issues relating not only to freedom and regulation but also to child protection. On the contrary, its advantages are almost negated by its disadvantages. As discussed, its practical effectiveness is still very doubtful, while it involves controversial issues relating to freedom of expression. Indeed, it is questionable whether it is an appropriate regulatory method for dealing with harmful Internet content — illegal Internet content, such as child pornography, is beyond the scope of the rating system, because this kind of illegal content is "forbidden for any conceivable audience" and "should be regulated by the enforcement" of laws (Cyber-Rights & Cyber-Liberties (UK), 1997).

A report from Cyber-Rights & Cyber-Liberties (1998) tests whether the Internet content rating scheme meets the principles of good regulation which was published by the Better Regulation Task Force in January 1998. Through

the test, it identifies that the Internet content rating system 1) does not have broad public support; 2) may not be enforceable; 3) is not easy to understand, because of complex technical issues; 4) may bring unintended consequences, such as a chilling effect on freedom of expression; 5) is a response to a short-term public concern; 6) may create a false sense of security for concerned citizens, because of its technical defects; 7) may unconditionally prohibit harmful content that is freely available to adults in other media; 8) may not fulfill its public accountability, because of its industry-based nature.

The dissemination of harmful content on the Internet is a serious social concern that needs to be addressed. However, in my view, the filtering and rating systems do not seem to be appropriate solutions. As PCMLP (2004, p. 70) points out, Internet content filtering remains an area where self-regulation has raised far more concerns than solutions. If so, what can be the alternatives? GILC (1999) argues, "Approaches that emphasize education and parental supervision should receive far more attention." Akdeniz (2004, p. 120) also claims, "There should be more emphasis on promoting the Internet as a positive and beneficial medium and there is urgent need for awareness of Internet usage." As discussed previously, the role of Internet users in controlling harmful Internet content is crucial. Ultimately, parents and teachers have the prime responsibility for the protection of children from accessing potentially harmful content on the Internet. In this context, the EU Action Plan's awareness action line may be a desirable approach to Internet content regulation, but it's backing for filtering and rating systems may need to be reconsidered.

CHAPTER 6

DEVELOPMENT OF THE INTERNET IN SOUTH KOREA

6.1. Introduction: Wired South Korea

Before discussing the Internet content regulation and the Internet content rating system in South Korea, it is necessary in my view to understand its unique Internet environment. South Korea is remarkable in that it has established a very extensive Internet infrastructure and successfully pursued policies intended to make it a leader in terms of Internet usage. South Korea is the first country in the world which has adopted the broadband Internet connection nationwide (see Chapter 6.1.3).[1] South Koreans also spend the longest time online worldwide (see Chapter 6.1.2). Korean style Internet cafés, the so-called PC BANG (literally, room), are everywhere on the high street. Fulford (2003) calls South Korea the world's most wired nation in his article published in Forbes Magazine, *Korea's Weird Wired World.*

From politics and media to entertainment, South Korean society has been reshaped by the Internet. In summer 2002 a small online community of football supporters, Red Devil, organised millions to take to the streets to cheer on the national football team's World Cup match (Yoo, 2002; Lee & Kang, 2001). In November 2002 a netizen, Kim Ki-bo, posted an article on the Internet which broached the idea of holding candlelight vigils to mourn the girls who were crushed to death in June 2002 by an armoured vehicle operated by two US soldiers (D. Lee, 2002). This article quickly spread out and raised public resentment. Beginning the end of November, a growing number of people have taken part in a daily candlelit vigil in GWANGHWAMUN, central Seoul, to mourn the two girls. Since then, tens of thousands of protesters also marched in other major cities, including BUSAN, DAEGU, GWANGJU and ULSAN (Ji H. Kim,

[1] In 2000 the South Korean government completed the nationwide broadband network which linked 144 major cities. As early as 2001, the government has provided remote mountain or island villages with the broadband Internet connection through its artificial satellite, Mugunghwa (literally, the rose of Sharon. South Korea's national flower) (NCA, 2001, p.85).

2002). The result of the presidential election in December 2002 confirmed that the emergence of new media centred on the Internet has fundamentally changed the journalistic environment (Rhee, 2003). The established media were stunned by the explosive power of the Internet media and netizens who dominated the campaign. During the campaign the most popular and influential media were not traditional newspapers, but Internet newspapers, such as *OhmyNews* (H. J. Kim, 2003, pp. 94-95; Lee & Kim, 2003: pp. 37-39). Everyday, millions of people exchanged their opinions and news via these Internet newspapers and several major portal sites, such as NAVER and DAUM (J. W. Han, 2003). And then netizens' power made history on the presidential election day.

> By 11 a.m. on Dec. 19, exit poll results showed that the iconoclastic Roh Moo Hyun, 56, a 2-to-1 favorite among youth, was losing the election. His supporters hit the chat rooms to drum up support. Within minutes more than 800,000 e-mails were sent to mobiles to urge supporters to go out and vote. Traditionally apathetic young voters surged to the polls and, by 2 p.m., Roh took the lead and went on to win the election (Fulford, 2003).

Roh won the election by a narrow margin of 2.5 percent. South Korean media names it a victory of Internet election ("INTERNETSI IRWONAEN," 2002). Lee and Kim (2003) argue that although political effects of the traditional mass media should not be underestimated, the Internet significantly affects the political participation of voters, in particular young people in their twenties and thirties. Professor Han Jong-Woo (2003) argues that "cyberspace as a new information age public sphere is liberating the young generation from hierarchical and authoritarian political structures" in South Korea.

Indeed, in South Korea the Internet has had a very substantial impact, certainly its impact is greater than has been the case in most other countries in the world.

In this chapter its significant Internet usage and infrastructure will be explored. A number of factors relating to the explosive development of the Internet, ranging from cultural aspects to government policy, will be discussed.

6.1.1. The Number and Ratio of Internet Users

The number of Internet users is one of the key indicators for assessing the degree of development of the Internet. However, there is no international single measure for this. Therefore, it can vary according to each statistical agency. For this study statistics from a governmental institution, the Korean Network Information Centre (KRNIC), were mainly employed. These are the South Korean government's official statistics. Here, Internet users mean people who are six years old or over and use the Internet once a month or more.

According to a report from the KRNIC (2003), over the last few years the number of Internet users in South Korea has been increasing at breakneck speed. Between 1997 and 2002 the number increased 16 times from 1.634 million to 26.27 million. In particular, during 1998 and 1999 it recorded remarkable rates of increase, 90 and 250 percent respectively. By December 2002 the number of South Korean Internet users ranked sixth in the global country ranking of Internet users, while its total population ranked 26th in the world (UN Population Division, 2003).

However, the large number of Internet users does not necessarily mean a high ratio of Internet users in the entire population. For instance, China's 59.1 million Internet users accounts for only 4.7 percent of China's entire population.[2] By December 2002, its ratio of Internet users ranked sixth in the

[2] The population of China had reached 1275 million by 2000 (UN Population Division, 2003).

world, as did its Internet population (KRNIC, 2003). By the same date there were 17 countries where the ratio of Internet users is higher than 50 percent. Iceland takes first place with 69.8 percent, followed by Sweden, Denmark, the Netherlands and Hong Kong. However, none of these five leading countries are ahead of South Korea in terms of Internet population (KRNIC, 2003). Therefore, these statistics prove that South Korea is one of the leading nations both in terms of Internet population and in terms of ratio of Internet users.

6.1.2. Time Spent Online

Another significant feature of Internet usage in South Korea is that South Koreans spent more than twice as much time online than most countries. According to the Nielsen//NetRatings (2001a), "South Koreans spend the most time surfing per month and the most time online per surfing session, with a surprising 16 hours and 17 minutes per month and 46 minutes and 25 seconds per session." The runners-up, the Canadians, spent 10 hours and 48 minutes per month, which was about five hours less than South Koreans. This unique Internet usage is closely related to its high penetration of broadband Internet access.

6.1.3. The Broadband Internet Service

Apart from these noticeable features concerning Internet usage, South Korea has also established a very extensive Internet infrastructure. South Korea is the leading country in terms of broadband access to the Internet in the world. A report from OECD (2003) reported that by June 2002 South Korea took first place again with 19.1 broadband subscribers per 100 inhabitants. Canada was a distant runner-up with 10.2 subscribers per 100 inhabitants. The ratio of South Korean broadband subscribers is five times bigger than the average ratio of

OECD countries' and over eight times bigger than the average ratio of the European Union countries'.

Since broadband Internet services became available in South Korea, the number of broadband subscribers has increased faster than ever. According to statistics from the Ministry of Information and Communication (MIC),[3] during the two years between June 2000 and June 2002, the number multiplied six times from 1.5 million to 9.2 million. By December 2004 the number grew to 11.9 million (Y. K. Kang, 2005, p. 29)

This incredible popularity of broadband Internet services is based on a substantial infrastructure. By December 2000 the South Korean government linked 144 major cities with fibre optic cables, completing the first nationwide broadband network in the world. Through this network Korea Telecom could offer DSL services to 92 percent of the South Korean population (D. Kim, 2002; OECD, 2001). The South Korean government has invested 11 trillion KRW (about 5.1 billion GBP) on the broadband Internet network (H. Kim, 2002). Furthermore, the tariff of broadband Internet services is very low as compared to the UK and any other nations. For instance, As of January 2004, 2Mbps broadband Internet access is available at an average fixed line service charge of around 13 GBP per month in South Korea. 10Mbps broadband Internet access is also available for about 16 GBP.[4]

Alongside these outstanding governmental efforts, South Korea's unique

---

[3] The Broadband Network Division of MIC (Retrieved July 7, 2003, http://infonet.mic.go.kr/).

[4] The tariffs of broadband Internet services were surveyed from four ISPs Websites: Thrunet (http://www.thrunet.com), Hanaro Telecom (http://www.hanaro.com), Onse Telecom (http://sshark.shinbiro.com) and Korea Telecom (http://www.megapass.net) on 20th January 2004.

housing pattern with nearly 40 percent of the population living in high-density apartment blocks (Korea National Statistical Office, 2000)[5] allows for the easy deployment of broadband Internet networks. As a result, South Korea became the very first country in the world to adopt the broadband Internet nationwide.

6.2. Analysis: Factors of Internet Development in South Korea

South Korea, therefore, is remarkable in that it has established a very extensive Internet environment. Indeed, South Korea is one of the most wired places on the planet. These significant developments of the Internet in South Korea can be explained by a number of reasons ranging from socio-cultural factors to technical factors.

6.2.1. Socio-Cultural Factors

6.2.1.1. The Quick-Quick Culture

Firstly, it is a unique cultural characteristic of South Korean society that there is a general obsession with doing everything very fast. Doing things at high speed is common not only in the workplace, but even in restaurants. Indeed, South Korea is often dubbed a 'quick-quick culture.' One of the implications of this is that new trends tend to be adopted very fast and spread throughout

[5] Households by type of housing units (unit : million)

	Detached dwelling	Apartment building	Terrace house, Apartment unit in a private house	Dwelling units in the building not intended for habitation	Total
Number of household	7.103	5.238	1.294	0.593	14.227
Ratio	49.9 %	36.8 %	9.1 %	4.2 %	100.0 %

(Resource: Korea National Statistical Office, 2000)

society at lightening speed. As Jeffrey Jones[6] argues, the speed with which Koreans have taken to the Internet is an excellent example of this social trend (Seo, 2003, p. 103).

6.2.1.2. A Confucian Ethic Society

Secondly, South Korean society is still permeated by a conservative Confucian ethic which requires high standards in public life. Professor Jeon Tae-Guk (2002) draws a distinction between 'the Confucian system' which was a political idea of the ruling class in the traditional era and 'the Confucian everyday consciousness' which consists of the conscience, values, attitudes, customs and the forms of interaction of the people. Jeon argues that in contemporary South Korean society, Confucianism as a political ideology is a relic of the feudal times, but the Confucian ethos deeply influences people's everyday lives. As Jeon (2003) insisted, Confucian principles include obedience to an authority, emphasis on identifying harmonious relations rather than individual differences and respect for education. In this context, Macintyre (2000) says that in South Korea "the anonymity and freedom of cyberspace has provided an escape from old-style mores that many find oppressive, especially the youth." Ra Do-Sam (2003, p. 107) also argues that the Internet has offered a space where people can behave willfully regardless of hierarchical social relations.

Furthermore, Professor Shim Young-Hee (2001, p. 133) argues that until the late 1980s, "sexuality was not believed to be a proper topic of discussion or even of casual talk. It was almost a taboo." Shim claims (p. 137) that although

---

[6] Jeffrey Jones is a former chairman of the American Chamber of Commerce in South Korea and the author of the book, *NANEUN HANGUKI DURYEOPDA* (*I am afraid of Korea*) (2000, JUNGANG M&B: Seoul).

there has been a sweeping change in people's attitudes toward sexuality with industrialization, urbanization and Westernization, some of Confucian discourses and ideologies linger in contemporary South Korean society, particularly the double standard of sexuality — while the informal sexual systems for men, such as female prostitution, flourish, chastity is still stressed as the greatest of womanly virtues. Thus South Korea's social customs have made the public uneasy to expressing or consuming sexual desires. However, this sexual conservatism has been quickly shattered by the advent of the Internet, since it enables people to access so-called adult information in strict privacy and in an anonymous manner. Ra (2003, p. 110) argues that ironically this social philosophy which oppresses sexuality has greatly assisted the adoption of the Internet in South Korea.

Here is a prime example. In March 1999 a Korean top actress' sex video was revealed to the public. In fact, she was a famous conventional actress and by no means a porn star. Her ex-boyfriend sold, without her knowledge or permission, a salacious video made for entirely private purposes. In South Korea, usually, these kinds of videos are sold on the black market. However, in the Internet era it has become a different story. The actress' video, as a form of computer file, instantly spread throughout the Internet hundreds of times faster than any conventional distribution methods. This controversial event scandalised South Korean society. Surprisingly, many people joined a broadband Internet service to download the hundred mega-bites video file. Even computer-illiterates rushed to get on to the Internet. Thereafter, downloading such kinds of files became hugely popular (H. Kim, 1999; Struck, 2000). Although this incident was an intolerable intrusion which completely destroyed a human being's privacy and clearly showed an ill effect of the Internet, ironically it is often considered an important catalyst for the popularisation of the Internet in South Korea (Moon, 2003, p. 354).

6.2.1.3. Enthusiasm for Education

Thirdly, the high priority afforded to education has accelerated the shift towards an Internet-centred society. Since September 2000 the South Korean government has offered free broadband Internet services to every primary, middle and high school. According to a report from the National Computerisation Agency (NCA), *2002 Korea Internet: White Paper*, 99.3 percent of University students, 99 percent of high school students, 99.8 percent of middle school students and 88.4 percent of primary school students were Internet users as of December 2001. Furthermore, the most popular reason for the first use of the Internet was educational purposes. "School assignment" was the first reason with 16.4 percent. "Children's education" was fifth with 9.1 percent. These educational purposes amounted to over 25 percent and were ahead of "general information search" and "business use." (NCA, 2002)

6.2.1.4. The Internet PC "BANG" Culture and Online Games

Another important reason for the successful development of the Internet is the phenomenal boom in the Korean version of the Internet café, so-called Internet PC-BANG (literally, PC room). A PC-BANG is a shop, open 24-hours-a-day, where people gather to surf the Internet for e-mailing, online Internet chatting, online stock trading and, in particular, playing network games such as the hugely popular StarCraft and Lineage. At the end of 1997 several PC-BANGs opened mainly around universities in Seoul, the capital of South Korea. PC-BANGs immediately won popularity and became the second most popular place for Internet access (NCA, 2002, p.63), and its business has quickly grown into a huge market. Its revenues reached 1.65 trillion KRW (about 870 million GBP) in 2003 ("OLHAE GUKNAE", 2003). Despite around 60 percent of South Korean households having Internet access via their home PCs as of 2002

(Nielsen//Rating, 2002), PC-BANGs are still enjoying high popularity, because PC-BANGs are inexpensive,[7] convenient and provide faster Internet access with high performance PCs — they usually allow smoking and drinking.

Alongside the phenomenal boom in the Internet PC-BANG, the huge popularity of online games among the young is also one of the major reasons for the successful development of the Internet in South Korea. The online game fever has resulted in the speedy growth of PC-BANGs. Through PC-BANGs, online games have grown in popularity. As more and more Korean youth enjoy the game, buying and selling online game items for real money is a very common practice. Even cyber money, the so-called 'Adena,' can be exchanged for real money at the rate of ten 'Adena' to one KRW.[8] For instance, on Lineage a 'Ring of Teleport Control' and 'Power Gloves' are trading at 300 GBP and 670 GBP respectively over the Internet. In order to attain the highest level of Lineage, the 'Lord of Castle,' a cyber castle is needed. Outrageously, it is trading at about 17,000 GBP. There are a number of trading and auction sites, such as Itembay.com, which deal only with online game items.

However, behind their explosive popularity there are also some extremely negative influences at work. Crimes that are related to these games have increased enormously and are still increasing. In 2001 over 1,000 people, including teenagers, were accused of fraud related to the trading of Lineage items. In March 2001 a high-level gamer was robbed of his all Lineage items which were worth about 6,000 GBP. A month later, another player was arrested for violence toward his online game rival ("Online game," 2002). Subsequently, many similar incidents followed. Unfortunately, these kinds of

---

[7] The tariff of PC-Bangs starts from around 50 pence per hour, but differs from region to region. The national average is about 80 pence per hour.

[8] KRW is the currency unit in South Korea.

incidents are by no means unusual in South Korea. Despite the bad influence of online game culture, the online game market in South Korea is growing rapidly. In 2004 the revenues of online games in the South Korean market reached 1.09 trillion KRW (about 573 million GBP) ("JEONGBO TONGSINUI NAL", 2005).

6.2.2. Internet Policy

In addition to the above-mentioned socio-cultural factors, in terms of public policy, the South Korean government has strongly promoted Internet usage and established a very extensive Internet infrastructure. Since the 1960s, South Korea has developed into an industrial nation by successfully implementing foreign industrial technologies to achieve accelerated growth. As a result, South Korea has been one of the fastest-growing nations in terms of industrial development in the world and is now a member of the Organisation for Economic Development and Cooperation (OECD). However, a severe economic crisis hit South Korea in December 1997. Extremely high foreign exchange rates and Interest rates suddenly struck South Korea. South Korea received bailout funds from the International Monetary Fund (IMF). To comply with the IMF programme,[9] companies carried out radical restructurings (Euh, 1998). Most Koreans feel that this was the most critical economic crisis nationwide since the 1950s, and the period is referred to as the 'IMF era' (Yoon, 1998, pp.149-150). In August 2000, as the Executive Board of the IMF completed the final review of Korea's economic reform programme (IMF, 2000). By August 2001 South Korea completed its repayment of the full amount of loans from the IMF (19.5 billion USD) (IMF, 2001). South Korea's financial crisis was officially over. However, it has deeply influenced almost

[9] see IMF Stand-By Arrangement Summary of the Economic Program (December 5, 1997). The full text is available on the IMF Website at http://www.imf.org/external/np/oth/korea.htm (Retrived March 30, 2005).

every sphere of South Korean society, in particular the overall structure of the economy (D. J. Jang, 2003).

Since the IMF era, the greatest challenge for South Korea has been to improve its national competitiveness by restoring its growth potential, and by creating an environment conducive to rebuilding economic vitality. The South Korean government has recognised that this restructuring can best be achieved through the creation of a strong knowledge and information-based economy (MIC, 1999b).

The World Bank emphasised in its report, *World Development Report 1998-99: Knowledge for Development*, that the core elements necessary for a nation to achieve economic development are greatly dependent on the creation, diffusion and utilisation of knowledge (World Bank, 1998). Indeed, during the last decade, rapid advances in information technology (IT) have quickly turned the global economy into a knowledge-based economy where information and knowledge are the prime sources of value-added. In a knowledge-based economy,[10] accumulation and the effective utilisation of knowledge and information, rather than a huge input of capital and labour, largely determine economic development. Therefore, a nation's competitiveness will be dependent on institutional, cultural and technological environments for creating value-added through the accumulation, dissemination and utilisation of knowledge and information.

In 1995 the South Korean government enacted *JEONGBOWA CHOKJIN GIBON*

[10] OECD defines the term 'Knowledge-based Economy' as an economy which is directly based on the production, distribution and use of knowledge and information (OECD, 1996).

BEOP [*Framework Act on Informatisation Promotion*][11] and instituted a public fund for promoting the communication and information industry. 630 billion KRW (about 295 million GBP) in 1999, 560 billion KRW (about 262 million GBP) in 2000, and 578 billion KRW (about 271 million GBP) in 2001 were provided. In March 1999 the South Korean government stated, "*Informatisation* is the key national strategy for such environments" (MIC, 1999a) and launched the Cyber Korea 21 project that is the blueprint for becoming a leading nation in knowledge and information in the 21st century (MIC, 1999b). Cyber Korea 21 aimed to create the framework for a knowledge-based society and to improve national competitiveness and the quality of life up to the level of the world's advanced nations. The three key policies of the project were: *strengthening* the information infrastructure for the creation of a knowledge-based society, *increasing* national productivity by utilising the information infrastructure and *promoting* new businesses based on the information infrastructure. Firstly, in order to strengthen the information infrastructure, the government planned to upgrade telecommunication networks through establishing a nationwide high-speed optical fibre backbone connection and to fund a number of IT projects and businesses. An information education plan targeting the entire population was also launched. Secondly, for increasing national productivity in the information age, the government planned to digitise the methods and procedures of administrative affairs. Thirdly, through the information infrastructure it promoted new businesses, in particular e-commerce, and encouraged the Internet industry to create new jobs (MIC, 1999c).

As a part of the project, the government has established a substantial

---

[11] Act No. 4969. The Act was last amended on 30th December 2004 (Act No.7265). The full text of the Act is available in English on MIC Website at http://www.mic.go.kr/ (Retrieved April 27, 2005).

infrastructure for broadband Internet connection and encouraged competition between Internet service companies in terms of their service quality, tariff and so on. Consequently, a very low tariff for Internet access has been available. (see Chapter 6: Footnote 4) The government also distributed low-priced PCs which are called 'Internet PC' (MIC, 1999c), in order to promote computer and Internet literacy, mainly targeting the low-income class. An Internet PC can be instantly purchased at any local post office for approximately 45 GBP, the first instalment of 'People's Computer Instalment Saving' scheme. Also, people can buy it from 12 official Internet PC vendors for cash or by credit card.

6.3. Internet Content Regulation Policy in South Korea

Therefore, the South Korean government has played a decisive role in developing the Internet, while in most other countries industries have taken on the task. The government-centred Internet policy has been very successful in establishing a substantial infrastructure and encouraging the Internet industry. However, in terms of Internet content regulation the South Korean government has not performed well at all.

In South Korea, before the Internet proliferated, the major online medium was the PC Tongsin (literally, communication). The PC communication service began in 1984 its subscribers reached about three million in 1998 — however, the PC communication services disappeared one by one, after commercial Internet services were initiated in 1994 (Internet Association of Korea, 2005). Consequently, the dissemination of explicit sexual materials through these online services emerged as a social concern and the government started to take action on this issue (W. Jeong, 2001). On 5th January 1995, soon after commercial Internet service began to be available in South Korea, the Korean National Assembly amended *JEONGI TONGSIN SAEOP BEOP* [*the*

Telecommunication Business Act][12] to establish a content regulatory agency for PC Tongsin and the Internet, JEONGBO TONGSIN YUNRI WIWONHOE [Information and Communication Ethics Committee].

After, during the year 1999, the number of Internet users recorded a significant 250 percent increase, in July 2000 the South Korean government introduced a mandatory Internet content rating system under the revised version of *JEONGBO TONGSINMANG IYONG CHOKJIN MIT JEONGBO BOHO DEUNGE GWANHAN BEOPYUL* [*the Act on Promotion of Utilisation of Information and Communication Network*],[13] the so-called *TONGSIN JILSEO HWAKRIP BEOP* [*Communication Order Establishment Law*]. The proposed Internet content rating system would be managed by the governmental institution, the ICEC, while the Internet content rating systems in most other countries, including the US, the UK and other European countries, has been conducted by non-governmental organisations. The Act also imposed a heavy penalty on almost every Internet information provider for mis-rating or non-rating. The Act was passed by the National Assembly with these punitive clauses in December 2000. Many civil organisations, such as the JINBO (literally, 'progress') Network Centre,[14] were highly critical of the South Korean government and were of the opinion that it is using its Internet content rating system as a means of censoring the Internet.

Why does the government introduce the mandatory Internet content rating system? The first answer may be found in the existing content regulatory

---

[12] see Chapter 7.1.2.

[13] see Chapter 7.1.3.

[14] The JINBO Network Centre, the so-called JINBO-net, has played a major role in the civil campaigns against governmental intervention on freedom of communication on the Internet in South Korea. It was launched in November 1998 as a centre for providing computer communication services, including Internet service and training services for South Korean NGOs, and as an independent non-profit organisation for action itself (Kang, 1998).

regimes of other media areas. In South Korea a number of governmental initiatives have conducted content regulation of each distinctive medium area (see Table 6.1). HANGUK GANHEANGMUL YUNRI WIWONHOE [Korea Publication Ethics Commission] has taken charge of content regulation in the printing area. Under Article 16 of *CHUPAN MIT INSWAE JINHEUNG BEOP* [*Publication and Printing Promotion Act*],[15] it conducts deliberation on publications including daily newspapers, books, magazines, comics and e-books. BANGSONG WIWONHOE [Korean Broadcasting Committee] has been responsible for content regulation in the broadcasting area under *BANSONG BEOP* [*Broadcasting Act*].[16] YEONGSANGMUL DEUNGGUK WIWONHOE [Korea Media Rating Board] of MUNHWA GWANGWANGBU [Ministry of Culture and Tourism] has regulated the area of motion pictures, video products and games, including online games.[17] The Information and Communication Ethics Committee (ICEC) is one of these governmental content regulatory agencies. It

---

[15] *The Publication and Printing Promotion Act* was enacted on 26th August 2002 (Act No. 6721). The full text of the Act is available in Korean on the Korea Publication Ethics Commission Website at http://www.kpec.or.kr/html/law_07/law01_01.asp (Retrieved March 31, 2005).

[16] *The Broadcasting Act* was enacted on 12th January 2000 (Act No. 6139). Articles 32, 33 and 34 of the Act are titled "deliberation on impartiality and public nature of broadcast," "deliberation rules" and "deliberation committee" respectively. The full text of *the Broadcasting Act* is available in English on the Korean Broadcasting Commission Website at http://www.kbc.go.kr/english/common/broadcating.asp (Retrieved March 30, 2005)

[17] The KMRB and its predecessors have been criticised for censoring films, sound records and other media (W. Han, 2003). In April 1997 GONGYEON YUNRI WIWONHOE [Performance Ethics Board (PEB)] was reformed and became HANGUK GONGYEON YEOSUL JINHEUNG WIWONHOE [Korea Performing Art Promotion Commission (KPAPC)], after the Korean Constitutional Court held the prior deliberation system under *YEONGHWA BEOP* [*Film Act*] (Act No.2536. Feb.16, 1973) unconstitutional on 4th October, 1996 (8-2 KCCR 212, 93Hun-Ka13), and subsequently declared unconstitutional against the prior deliberation systems on phonograph records (8-2 KCCR 395, 94Hun-Ka6, Oct. 31, 1996) and on video products (9-1 KCCR 267, 97Hun-Ka1, March 27, 1997) respectively. In February 1999 *EUMBAN MIT VIDEOMULE GWANHAN BEOPRYUL* [*Sound Records and Video Products Act*] was amended to *EUMBAN, VIDEOMUL MIT GAMEMULE GWANHAN BEOPRYUL* [*Sound Records, Video Products and Game Products Act*] (Act No.5925). According to the amendment, the KPAPC changed its name to the KMRB in June 1999 (W. Han, 2003; K. Kim, 2003; KMRB, 2002).

has played a major role in regulating comprehensive Internet content (see Chapter 7).

Type of Media	Deliberation Body	Ground Regulation	Objects of Deliberation	Type of Deliberation	Type of Rating
Printing	HANGUK GANHEANGMUL YUNRI WIWONHOE [Korea Publication Ethics Commission]	*CHUPAN MIT INSWAE JINHEUNG BEOP* [*Publication & Printing Promotion Act*]	Periodical, Book, Electronic Publication	Post-Deliberation	Harmful-to-youth material
Broad-casting	BANGSONG WIWONHOE [Korean Broadcasting Committee]	*BANGSONG BEOP* [*Broadcasting Act*]	Broadcasting	Post-Deliberation	All 7-years 12-years 15-years 19-years
Electronic Communi-cation Media	JEONGBO TONGSIN YUNRI WIWONHOE [Information & Communication Ethics Committee]	*TONGSIN SAEOP BEOP* [*Telecommuni-cation Business Act*]	Information that is published and distributed to the public through telecommunicati ons line	Post-Deliberation	Harmful-to-youth material
Film, Video, etc.	YEONGSANGMUL DEUNGGUKWIWON HOE [Korea Media Rating Board]	*EUMBAN, VIDEOMUL MIT GAMEMULE GWANHAN BEOPRYUL* [*Sound Records, Video Products & Game Products Act*]	Sound Records	Post-Deliberation	All 18-years
			Video Products	Prior Deliberation	All 12-years 15-years 18-years
			Game Products	Prior Deliberation	All 18-years
		YEONGHWA JINHEUNG BEOP [*Film Promotion Act*]	Film	Prior Deliberation	All 12-years 15-years 18-years Restricted
		GONGYEON BEOP [*Performance Act*]	Performance	Post-Deliberation	All 18-years

Table 6.1. The content rating system in South Korea (Hwang & Hwang, 2003, p. 250)

As presented in Table 6.1, these content regulatory agencies primarily regulate content by giving a certain rating. Under *the Broadcasting Act*,[18] a broadcasting company must monitor the content and provide a rating in advance, and must show the applicable grade on the top of the right side of the screen at the time of broadcasting. KMRB rates films, videos, games, performances, phonogram and advertising products by age, based on *the Film Promotion Act*; *the Sound Records, Video Products and Game Products Act* and *the Performance Act* (K. Kim, 2003).[19]

In this context, Professors Hwang and Hwang (2003, pp. 248-249) argue that content regulation in South Korea is based on rating systems which comply with prior and post-deliberation of governmental agencies. At this point, I do not entirely deny the necessity of these deliberation systems. As discussed in the previous chapter, broadcasting media is subject to strict governmental regulation (see Chapter 2.7). Most countries have a voluntary or forcible rating system for films and video products (W. Han, 2003, p. 110),[20] but the South Korean government attempted to apply these regulatory strategies to content on the Internet.

Secondly, under this regulatory tendency, the governmental agencies, the South Korean National Computerisation Agency (NCA)[21] and ICEC have developed Internet content filtering and rating measures as early as 1997. As discussed in

---

[18] see Chapter 6: Footnote 16.
[19] see Chapter 6: Footnote 17.

[20] In the UK, the British Board of Film Classification (BBFC) which is an independent, non-governmental body has exercised its rating system on films since 1913 and on video materials since 1985 (Resource: BBFC Website. http://www.bbfc.co.uk/, retrieved March 31, 2005).

[21] The National Computerisation Agency was established in 1986 under *JEONGI TONGSIN GIBONBEOP* [*Framework Act on Telecommunications*].

Chapter 4, Internet content filtering and rating technologies have been developed by commercial companies or non-governmental institutions. In South Korea the government has initiated the development of such technologies (see Chapter 7.2). ICEC launched a project for developing the Korean Internet content rating system in 1997. Two years later, ICEC presented the prototype of its own system which was called the ICEC Internet content rating system (ICEC, 1999).

In this context, introducing the mandatory Internet content rating system in 2000 was not a sudden incident, but an extension of the existing rating regimes. However, the Internet environment is significantly different to other traditional media. The Internet is a global medium which cannot come under a single nation's rating regime. In the next chapter I will explore the Korean Internet content rating system and discuss its serious drawbacks.

CHAPTER 7

THE INTERNET CONTENT RATING SYSTEM IN SOUTH KOREA

7.1. The Internet Content Regulation in South Korea

In the previous chapter I discussed the significant development of the Internet in South Korea and the South Korean government's considerable role in that. As discussed in the previous chapter, the European Union has adopted a multi-layered co-regulatory approach to Internet content regulation. While, as regards illegal content, law-enforcement authorities have held a prime responsibility, self-regulatory solutions have been employed for dealing with potentially harmful content (see Chapter 3.7). However, the South Korean government strongly dominates regulation of both illegal content and harmful content on the Internet. It has been criticised by a number of civil organisations, such as the JINBO Network Centre, since it has constantly raised censorship issues. In the next section, in order to understand Internet content regulation in South Korea, two major laws, *JEONGI TONGSIN GIBONBEOP* [*Framework Act on Telecommunications*], and *JEONGI TONGSIN SAEOPBEOP* [*Telecommunication Business Act*] will be discussed. The focus will then shift on to *JEONGBO TONGSINMANG IYONG CHOKJIN MIT JEONGBO BOHO DEUNGE GWANHAN BEOPYUL* [*Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.*] which has been extremely controversial in its introduction of a compulsory Internet content rating system.

7.1.1. JEONGI TONGSIN GIBON BEOP [Framework Act on Telecommunications] [1]

The Framework Act on Telecommunications was wholly amended in 1991 (Act No. 4393) in order to provide basic guiding principles on telecommunications (Article 1) and ministerial authority regarding promotion of

[1] The Act was last amended on 26th December 2002 (Act No. 6823). The full text of the Act is available in English on MIC Website at http://www.mic.go.kr/ (Retrieved April 27, 2005).

telecommunications technology and technical standards for telecommunications facilities (Article 5). Significantly, it also imposes penalties for false and obscene communications. Article 47 of *the Framework Act on Telecommunications*, which was revised in December 1996, prescribes that a person who communicates false information with the intention of violating public interests can be sentenced to up to five years' imprisonment or punished with a fine of up to 50 million KRW (about 27,000 GBP). The same Article also rules that a person who communicates false information with the intention of looking to one's own or another person's interests, or with the object of violating another person's interests can be sentenced to up to three years' imprisonment or punished with a penalty up to 30 million KRW (about 6,500 GBP).

Article 48(2) of this Act which was newly added in December 1996 stipulates that a person who distributes or sells obscene information can be sentenced to up to one year's imprisonment or punished with a fine of up to 10 million KRW (about 5,400 GBP). This Article is based on Article 243 of *Criminal Law* which regulates obscenity in the print media and is now being used as a comprehensive authority for dealing with cyber pornography (Park, 2000). The first legal case to which Article 48(2) applied was brought two years after it had been enacted. The Seoul District Court punished a person who posted nude pictures of a famous Korean nude model, Lee Seung Hee, with a penalty of two million KRW (about 1,100 GBP) for infringing Article 48(2) of *the Framework Act on Telecommunications* on 29th September 1998 (Hwang, 2000). As discussed in Chapter 2.5, in South Korea a number of precedents have set up jurisprudence of obscenity. However, the South Korean Court's obscenity test has been criticised for being based on conservative morality rather than any other standards, such as artistic merit or ideology.

Here is a prime example which shows the South Korean prosecution's arbitrary interpretation of what constitutes obscene materials. On 26th May 2001 an art teacher at Bee-In Middle School, Kim In-Kyu, was arrested for posting his and his pregnant wife's nude picture on his own cyber gallery site. At the same time his Web hosting company closed down his Website according to the Information Communication Ethics Committee's (ICEC) order (Y. Oh, 2001). He was indicted for violating *the Telecommunication Business Act*, but was released on bail two weeks later (G. Lee, 2001a). Ironically, on the same day Kim was arrested, many major newspapers in South Korea, including the Hankyereh, printed Spencer Tunick's[2] photograph of 2,000 naked people lying down on the Montreal Art Centre's stairway. No authority discussed whether this constituted obscenity (J. Jeong, 2001). On 18th June, CHUNGCHONGNAMDO Office of Education suspended Kim In-Kyu from school (G. Lee, 2001b). This incident sparked off contentious debates on obscenity on the Internet. On 14th June, 34 civil organisations, including the People's Artist Association, the Citizen's Coalition for Democratic Media and the Korea Cartoonists Association, issued a statement which criticised the prosecution's prejudice against obscene materials and supported Kim's belief about art (Song, 2001). Professor Baek (2001) claims that this case was the prosecution's witch-hunting for justifying its Internet censorship. He also criticises that the ICEC closed down Kim's site without any due process. In December 2002 the DAEJEON District Court found Kim In-Kyu not guilty.[3] The Court referred to the *Happy Sara* case[4] and stated that although the art works which Kim In-kyu

---

[2] Spencer Tunick is an artist who has been documenting the live nude figure in public, with photography and video, since 1992.

[3] Judgment of Dec. 27, 2002, 2001Go-Hap54, DAEJEON JIBANG BEOPWEON, HONGSEONGJIWEON HYEONGSABU [Daejeon District Court Hongseong Branch Court Criminal Department]

[4] 94DO2413, see Chapter 2: Footnote 31.

posted on his Website contain some explicit sexual depictions, they surely have "artistic values" and therefore did not appeal to the public's "prurient interest" and not affront "an average person's proper sense of shame about sex."[5] Many civil organisations, including the JINBO Network Center welcomed the decision and appraised that it is significant in that the Court emphasised "artistic value" and "freedom of expression" than any other factors when it examined whether Kim's works on the Internet was obscene (INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE, 2003, pp. 238-240). Indeed, it presented a contrast to the previous Supreme Court cases, such as the *Happy Sara* case and the *Lie to me* case,[6] which considered artistic value only as one of many points to be taken into account in its obscenity test (see Chapter 2.5).

7.1.2. JEONGI TONGSIN SAEOP BEOP [Telecommunications Business Act][7]

The Telecommunication Business Act was wholly amended on 10th August 1991 (Act No. 4394) in order to regulate the following issues; licensing criteria and reporting procedures for telecommunications service providers (from Article 4 to Article 28); rights of telecommunications service users (from Article 29 to Article 33-3); telecommunications service providers competition safeguards (from Article 33-4 to Article 38); construction and maintenance of telecommunications facilities (from Article 39 to 52).

Article 53(3) of *the Telecommunications Business Act* relates to the Ministry of

---

[5] 2001Go-Hap54. see Chapter 7: Footnote 3.

[6] 98Do679, see Chapter 2: Footnote 33.

[7] The Act was last amended on 31st March 2005 (Act No. 7445). The full text of the Act is available in English on MIC Website at http://www.mic.go.kr/ (Retrieved April 27, 2005).

Information and Communication (MIC) Minister's refusal, suspension, and restriction order against "improper communications." A person who does not comply with the order can be sentenced to up to two years' imprisonment or punished with a fine of up to 20 million KRW (11,000 GBP). Furthermore, Article 53(2) provides the legal foundation of ICEC and its content's deliberation system.

ICEC has implemented a monitoring system to prevent illegal activities or harmful information from being distributed. Two hotlines, which are named the "Internet 119" and the "Cyber Defamation and Sexual Violence Counseling Centre," have been established to assist users in filing complaints (ICEC, 2003). It has exercised considerable power and played an important role in regulating content on the Internet. Ironically the government and ICEC itself insist that ICEC is an independent organisation. It is widely argued that ICEC is an administrative organisation under the aegis of MIC (S. Lee, 2001). According to Article 53(2) of *the Telecommunication Business Act*, all board members of ICEC are appointed by the MIC Minister. Under Article 16(5) of *Enforcement Decree of Telecommunication Business Act*[8] ICEC should report its operations to the MIC Minister within 20 days. Article 16(4) of the same Enforcement Decree provides an authority for requesting of revision against "improper information." Although ICEC's order is only administrative, it effectively imposes a judicial power, since ICEC is legally obliged to ask the MIC Minister to exercise the Minister's refusal, suspension and restriction order which imposes a heavy penalty; either a maximum of two years' imprisonment or a fine of up to 20 million KRW (about 11,000 GBP). Furthermore, it is dependent on government funding. In the year 2001, the government paid

[8] The *Telecommunication Business Act Enforcement Decree* was last amended on 10th May 2004 (Presidential Decree No. 18388). The full text of the Enforcement Decree is available in Korean on MIC Website at http://www.mic.go.kr (Retrieved April 27, 2005).

ICEC's entire budget of 4.1 billion KRW (about 2.25 million GBP) (K. W. Cho, 2000). ICEC has been criticised for being a governmental censorship body. I will discuss this issue in more depth later in the chapter.

7.1.2.1. Unconstitutionality of Article 53 of the *Telecommunications Business Act*

While *the Framework Act on Telecommunications* imposes direct criminal punishments, *the Telecommunications Business Act*'s regulation system relies on administrative actions and ICEC's deliberation system. However, Article 53 of *the Telecommunications Business Act* is highly controversial for many reasons. First of all, it is strongly criticised for its obscure concept of improper communications. Article 16 of the Enforcement Decree defines "improper communications" as follows:

> Telecommunications which are deemed to be harmful to the public peace and order or social morals and good customs under Article 53(2) of the Act shall be as follows: (i) Telecommunications with contents that aim at a criminal act or of that abet a criminal act; (ii) Telecommunications with contents that aim at committing the anti-state activities; and (iii) Telecommunications with contents that impede the good customs and other social orders.

As Professor Hwang (2000, pp. 144-146) claims, in these definitions the meanings of "public peace and order" and "social morals and good customs" are not clear at all. Because they are very abstract concepts, they can be interpreted in a number of different ways according to a variety of political, religious and cultural viewpoints. Therefore, legislation which regulates the freedom of expression should be clearly circumscribed and unambiguous. However, as it stands the law is so vague that it enables the government to interpret it at will. There is no clarity or consistency and therefore injustices

may easily occur. From the individual's point of view, the comprehensive nature of the law is likely to result in severe self-censorship. This issue eventually brought a Constitutional Court case.

On 11th August 1999 a constitutional complaint was filed against Article 53 and parts of Article 71(vii) concerning Article 53(3) of *the Telecommunications Business Act* as well as Article 16 of *the Enforcement Decree of Telecommunications Business Act* (14-1 KCC 616, 99Hun-Ma480, June 27, 2002). The complainant, Kim Sun-Wook, claimed that these provisions violate the freedom of speech, the freedom of learning and art and lawful procedures which are provided by the Constitution of Republic of Korea Article 21, Article 22(1), and Article 12(1) respectively. He was a student of HANKUK Aviation University who joined NOWNURI, one of the major Korean computer networks, in his user identification (ID), IIJEAGI (literally, making an objection). On 15th June 1999, the plaintiff posted an article, entitled *SEOHAEAN CHONGGYEOKJEON EOSEOLPEUDA Kim Dae-Jung!* [*Yellow Sea battle, sloppy President Kim Dae Jung!*], to the bulletin board of CHANUMUEL (literally, cold well) community which is hosted by NOWNURI. A week later the NOWNURI system operator deleted the article without his consent and suspended his user ID for one month, in order to comply with the MIC Minister's administrative order. The plaintiff was given a one-sided notice without even being given any opportunity to defend himself. Thereupon, the plaintiff argued that Article 53 of *the Telecommunication Business Act* and Article 16 of *the Enforcement Decree of Telecommunication Business Act*, which authorises to the MIC Minister's order, had violated the constitution. On 11th July 1999 the plaintiff filed a petition. Almost three years later, in June 2002, the Korean Constitutional Court ruled Article 53 of *the Telecommunication Business Act* as unconstitutional. The significance of the Court's decision which for the first time restrains the government-centred Internet content policy will be discussed in depth in

7.1.3. JEONGBO TONGSINMANG IYONG CHOKJIN MIT JEONGBO BOHO DEUNGE GWANHAN BEOPYUL [Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.] [9]

In addition to two previous legislations, *the Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.*, the so-called *TONGSIN JILSEO HWAKRIPBEOP* [*Communication Order Establishment Law*], was introduced in July 2000.[10] The proposed Act covered various laws concerning regulations on telecommunication networks, including *CHEONGSONYEON BOHO BEOP* [*Juvenile Protection Act*], *the Framework Act on the Telecommunications*, *the Telecommunications Business Act*, *JEONJA SANGGEORAE GIBON BEOP* [*Basic Law on Electronic Commerce*] and *JEONJA SEOMYEONG BEOP* [*Digital Signature Act*]. It emphasised the reinforcement of personal information protection and information and communication network security. It also emphasised the regulation of improper information.

However, the government has faced tough challenges since the revised Act was proposed. It empowered the government to regulate the communication and information industry and end-users. Article 38 stated commercial image and sound information providers' obligation to store their serviced information.

---

[9] The Act was last amended 30th December 2004 (Act No. 7262). The full text of the Act is available in English on MIC Website at http://www.mic.go.kr/ (Retrieved April 27, 2005).

[10] *Ibid.* Article 1 of the Act states its purpose as follows:

> [To] promote the utilization of information and communications networks, to protect the personal information of people utilizing information and communications services, and to build an environment in which people can utilize safely and healthily the information and communications networks with the aim of serving to improve the people's lives and enhance the public welfare.

Article 40(4) banned the distribution, sale and display of any obscene sign, text, sound and image. Under Article 76 a person who violates this Article could be sentenced to up to one year's imprisonment or punished with a fine of a maximum of 10 million KRW (about 5,500 GBP). The government even attempted to intervene in domain name disputes. Article 72 provides the authority to establish a governmental institution, the so-called Korea Domain Name Dispute Resolution Committee.

7.1.3.1. Article 31 and the Internet Content Rating System

Among the many controversial issues of the proposed Act, the most disputed point was the Internet content rating system. The proposed Act presented a mandatory Internet content rating system. According to Article 31, a person who provides harmful information to minors on the Internet should self-rate their information and display the rating.

For several reasons, opponents, such as the JINBO Network Centre, perceived the proposed Act's Internet content rating system as a governmental censorship system (Hong, 2001). Firstly, it proposed that it should be managed by a government institution, although the Internet content rating systems in most other countries have been conducted by non-governmental organisations. Secondly, under the proposed Act, rating Internet content was not a recommended option, but a legal requirement. In a sense this Article might sound reasonable in terms of child protection on the Internet. However, the article was clearly contradictory, because the notion of "harmful information" on the Internet is too vague. In the COPA (CDA II) case the US Court held that applying a concept of harmful-to-youth to the Internet could result in blocking a substantial amount of Internet content which is lawful to adults (see Chapter 2.6.1.2). The Korean Constitutional Court also states that, as regards content

regulation, the concept of regulatory object should not be ambiguous, abstract, or comprehensive. Otherwise, it may be resulted in the regulation of communication that should not be regulated and may lead to the violation of the rule against excessive restriction (14-1 KCC 616, 99Hun-Ma480, June 27, 2002). In fact, courts often find it very difficult to judge this kind of issue.[11]

Nevertheless, under the proposed Act all judgments concerning harmful information on the Internet were entirely dependent on the decisions taken by ICEC. According to Article 29, ICEC was able to require Internet service providers to stop providing services to people who do not rate their Internet content. Worse still, according to Article 33, anyone who thinks Internet content rating is inappropriate could require ICEC to re-examine the rating. Then ICEC could require the content provider to submit information relating to its rating, and order a revision of the rating. Ironically, since "anyone can require ICEC," it was possible that ICEC could require itself to re-examine any Internet content's rating. Consequently, ICEC was virtually able to control the rating of any Internet information which falls within the South Korean government's jurisdiction. Furthermore, the proposed Act imposed a heavy penalty for mis-rating or non-rating. According to Article 77, a person who mis-rates on purpose could be sentenced to up to three years' imprisonment or punished with a fine of 30 million KRW (about 16,500 GBP).

Another problem was found in Article 34 which required that all public institutions, including schools and libraries, must install Internet rating software on their terminals. As discussed in the *Loudoun County Library* case and the *CIPA* case (see Chapter 2.5.1 & 2.5.2). installing Internet content

[11] see Chapter 2.5: the *Happy Sara* case (94Do2413) and the *Lie to Me* case (98Do679). Also see Chapter 7.1.1: the *Kim In-kyu* case (2001Go-Hap54).

filtering software in public institutions has proved to be controversial. While the CIPA applies to public schools and libraries, Article 34 targets all the public Internet access points which youths may use, including the Internet café. In my view, the issues concerning whether Internet content rating software should be installed at a school should be decided by the school, not by the government. Installing Internet content rating software in libraries also raises issues of serious concern. Libraries are institutions not only for children and teenagers but also for adults so installing any content filtering software in libraries may violate adult users' freedom of expression.

Fierce criticisms from many civil rights organisations and Internet users were made regarding the proposed Act. On 26th August 2000, the MIC's Website encountered an online demonstration. Thousands of enraged Internet users simultaneously visited the MIC's Website and disrupted service for hours, apparently as part of a massive "virtual sit-in" protest — a form of demonstration. As a result, the MIC's Website shut down for approximately ten hours (Kwon, 2000).[12] On 20th September 2000, 27 civil organisations including the Young Men's Christian Association (YMCA) and the JINBO Network Centre issued a manifesto which argued for the repeal of the Act ("JEONGBO TONGSINBUUI TONGSIN", 2000). Subsequently, in October 2000, 24 civil organisations jointly set up the network of civil rights organisations called JEONGBO TONGSIN GEOMYEOL BANDAE GONGDONG HAENGDONG [United Action Group Against Information and Communication Censorship] (2001, pp.

[12] MIC insisted that its Website was hit by a distributed denial-of-service (DDOS) attack and accused the JINBO Network Centre for the incident, since an unknown user posted a JavaScript, which could generate a DDOS attack, to the JINBO Network Centre's bulletin board. On 29th August 2000 the Cyber Terror Response Centre of the National Police Agency served a seizure and search warrant on the JINBO Network Centre. Later on, it was revealed that MIC's claim was untrue. The main cause of the incident was the MIC Web server's technical fault (S. Oh, 2000). The "virtual sit-in" protest is absolutely legitimate in South Korea and by no means constitutes hacking (Jang, 2001, pp. 7-9).

58-60) which took part in the campaign against *the Communication Order Establishment Law*.

In accordance with public opinion the proposed Act was twice revised through public hearings and debates. It was finally revised by the Science, Technology and Telecommunication Committee of the National Assembly on 8th December 2000. The committee deleted controversial articles related to the Internet content rating system. This revision followed an expert report which the committee commissioned (Science, Technology, Information and Telecommunication Committee of the National Assembly, 2000). The report claimed that the proposed Internet content rating system posed a number of problems as follows (pp. 14-15): Firstly, since cyberspace is an area where freedom of expression should be secured, direct governmental intervention in cyberspace is not recommended and may raise a censorship issue. Secondly, it is contradictory to mandate the rating system in the name of self-regulation. Thirdly, the rating system cannot be applied to obscene materials which are hosted abroad. Therefore it may not be practical. Fourthly, it may be difficult to guarantee the rule of clarity, if content selection software's object, standard and method are decided by a Presidential Decree. These viewpoints largely reflected civil organisations opinions.

Finally, on 20th December the Act was passed by the National Assembly, but not the sections relating to the Internet content rating system, although some other disputed articles such as Article 72 (Domain Name Dispute Resolution) remained. This seemed to be the final dispute over the mandatory Internet content rating system. Civil rights organisations announced their victory.

7.1.3.2. Article 42 and the Indication Method for Harmful-to-youth Content on the Internet

However, this was not the end of the story. Surprisingly, the mandatory Internet content rating system has been revived through the Enforcement Decree of the Act. Article 42 of the final version of the Act rules that "harmful-to-youth" information on telecommunications networks should be indicated according to the Enforcement Decree. People who violate Article 42 can be sentenced to up to two years' imprisonment or punished with a fine of up to 10 million KRW (about 5,400 GBP) under Article 64 of the Act. Article 42 was originally provided by the *CHEONGSONYEON BOHO BEOP* [*Juvenile Protection Act*].[13] Previously there was no electronic indication method.

Nevertheless, in April 2001 MIC announced that in order to comply with Article 42 it intended to add an Article about compulsory "Internet content selection software" to the new Enforcement Decree at its public hearing (INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE 2003 p. 2). Civil rights organisations immediately made the criticism that introducing compulsory Internet content selection software would mean the revival of MIC's Internet content rating system. In May 2001 the preliminary Enforcement Decree was announced. It changed the term "Internet content selection software" to "electronic indication." A month later MIC announced the PICS-based rating system which is compatible with the harmful-to-youth information filtering software as the indication method for harmful-to-youth information (MIC notification 2001-89).[14] In July 2001 *the*

---

[13] In the Act the term "juvenile" means any person below nineteen years old. The full text of the Act is available in English on the Commission on Youth Projection Website at http://www.youth.go.kr/English/protection/law.asp (Retrieved March 1, 2005).

[14] CHEONGSONYEON YUHAE MACHAEMULUI PYOSI BANGBEOP GOSI [Notification of harmful-to-

Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc. was enacted. In the same month its Enforcement Decree was also enacted. Article 21 of the Enforcement Decree forces harmful-to-youth information providers to give an electronic indication of harmful-to-youth information. The same Article entrusts the electronic indication method to the MIC Minister.

On 29th June 2001 around 500 Korean Websites went on a four day strike against the compulsory Internet content rating system (Min, 2001). In October 2001 the United Action Group's activists went on a hunger strike one by one. It lasted 60 days (K. Kim, 2001). However, they failed to bring about a public consensus on Internet censorship. Since the MIC's Internet content rating system has been justified in the name of protecting minors, many civil rights organisations, in particular the women's movement and the education sector, were reluctant to express their opinion concerning the issue and it remains very controversial.

Ultimately, the Internet content rating system has been developed as a self-regulatory solution to deal with potentially harmful Internet content. Illegal content is not a scope of the rating system — It is primarily a matter of law-enforcement (see Chapter 2.4). For this reason, the rating system has been operated by non-governmental institutions, in particular Internet industry-based bodies. However, in South Korea the government takes charge of managing the rating system. As discussed in Chapter 6.3, the South Korean government exercises its regulatory power on all the types of media through a number of content regulatory agencies, such as the Korea Publication Ethics Commission

---

youth Medium material indication method]. The full text of the notification is available in Korean on MIC Website at http://www.mic.go.kr (Retrieved April 27, 2005).

and the Korea Media Rating Board. These bodies have employed each age-based rating system, alongside prior and post-deliberation. This common regulatory regime has also been applied to the Internet. However, it is doubtful whether such a single nation's rating regime can effectively work under the global environment of the Internet. In the following sections I will explore two different Internet content rating systems of the ICEC from a technical viewpoint. These will focus on examining their practical implementations.

7.2. Technical Review: Two Internet Content Rating Systems of the ICEC

While in other countries, such as the US, commercial companies have played a major role in developing Internet content filtering software, in South Korea a governmental agency, the South Korean National Computerisation Agency (NCA) and ICEC have taken on this task. In 1997 NCA developed the first Korean blacklist filtering software, NCA Patrol, and distributed the software free to the public via ICEC's Website. In December 1999 NCA released the new versions of NCA Patrol, NCA Patrol 1.5 and NCA Patrol Proxy 1.0. NCA Patrol 1.5 aimed to be installed on a PC in schools or homes in non-network environments. NCA Patrol Proxy 1.0 was designed for network environments. NCA Patrol worked with both the Microsoft Internet Explorer 4.x and the Netscape Navigator 4.x on Windows NT/98/95 platforms (ICEC & NCA, 1999). However, in 2000 NCA and ICEC suddenly stopped distributing NCA Patrol and decided to hand over the filtering software project to commercial companies. NCA Patrol is no longer available. Instead, ICEC has provided commercial filtering software companies with an "overseas unhealthy sites blocking list." By August 2004 there were 21 commercial Internet content filtering software products which were approved by ICEC.[15] — Under Article

[15] The list of ICEC approved Internet filtering software products is available on SafeNet Website at http://www.safenet.ne.kr/software/products.html (Retrieved April 3, 2005).

32(5) of *the Sound Records, Video Products and Game Products Act*, PC cafés must install software or other device which is able to block obscene materials on the Internet. A person who violates this provision can be punished with a fine of up to 50 million KRW (about 27,000 GBP). Libraries and schools are not legally obliged to install filtering software.[16]

In 1999 ICEC developed the prototype of its own rating system (ICEC, 1999; Min, Kim & Lee, 2004, p. 119). This system later named SafeNet (http://www.safenet.ne.kr). Apart from this self-rating system, ICEC is also in charge of the mandatory Internet content rating system, named the harmful-to-youth material indication system. Both systems are based on PICS standard and managed by the ICEC. Furthermore, both principally aim at protecting youth from accessing potentially harmful content on the Internet. However, they are significant different. While the SafeNet system is a conventional rating system which is based on individual users voluntary participation, the harmful-to-youth material indication system is a mandatory system which can imposes prison sentences on violators. The latter system is compulsorily applied to harmful-to-youth information providers.

7.2.1. The SafeNet Internet Content Rating System

The SafeNet Internet content rating system is based on PICS specifications in order to be compatible with other PICS-based rating systems abroad, in particular the RSACi rating system. ICEC states that its system largely relies on the technical specifications of the RSACi system. Strictly speaking, the

[16] The proposed bill of *Communication Order Establishment Law* (Article 34) once required that schools, libraries and all the public Internet access points must install rating software on their terminals. However, this Article was abolished in the final version of the Act.

SafeNet rating system can be called the Korea version of the RSACi system. Thus, its meta tag is also similar to RSACi's. For instance, the meta tag of SafeNet's label for a sample Website is as follows:

```
<META http-equiv="PICS-label"
content='(PICS-1.1 "http://www.safenet.ne.kr/rating.html"
l gen true[false] for "a sample URL" r(n 3 s 3 v 1 l 1 i 0 h 1))'>
```
[17]

The SafeNet system's descriptors are also prepared on the basis of the RSACi rating standard. The rating category is almost identical to RSACi's, except it has a newly added 'et cetera' category. This system rates Web content in four main categories: violence, nudity, sexual act and language on a scale of 0 to 4. The additional 'et cetera' category has no scale of levels. Instead, its value is decided according to whether the information comes under the category's descriptors: drug use stimulus, weapon use stimulus, gamble, drinking stimulus and smoking stimulus. If the information is applicable to the descriptors, its value will be 1. If it is not, its value will be 0. The SafeNet's rating standards are as follows (Table 7.1):

[17] n=nudity, s=sex, l=language, i=drug use stimulus, weapon use stimulus and gambling, h=drinking and smoking stimulus

	Nudity	Sexual act	Violence	Language	Etc.
LEVEL 4	Exposure of genitals	Sex crimes or explicit sexual acts	Cruel killing	Explicit sexual language	1. - Drug use stimulus - Weapon use stimulus -Gambling 2. - Drinking stimulus - Smoking stimulus
LEVEL 3	Nudity	Non-explicit sexual acts	Killing	Severe expletives	
LEVEL 2	Partial nudity	Clothed sexual touching	Injury	Coarse expletives	
LEVEL 1	Revealing attire	Passionate kissing	Fighting	Common expletives	
LEVEL 0	None of the above	None of the above	None of the above	None of the above	

Table 7.1. The SafeNet's rating standards (Resource: SafeNet)

Furthermore, ICEC provides the recommendation list by age for some parents and teachers who have poor computer skills and Internet literacy (Table 7.2).

Category	Violence	Nudity	Sexual act	Language
Allowed for all (Allowed for elementary school girls and boys)	Level 1	Level 1	Level 0	Level 0
Over 12 years old (Allowed for junior high school girls and boys)	Level 2	Level 2	Level 2	Level 1
Over 15 years old (Allowed for high school girls and boys)	Level 3	Level 2	Level 2	Level 2
Over 18 years old (Allowed for adults)	Level 4	Level 3	Level 3	Level 4

Table 7.2. ICEC Recommendation list by age (Resource: SafeNet)

One of the unique features of the SafeNet system is that ICEC executes the self-rating service for domestic contents and the third-party rating service for foreign obscene and violent contents. While domestic information providers label in accordance with rating standards given by ICEC and the label

information is provided to enable users to select and use on the Internet, ICEC built the third-party rating database for foreign obscene and violent contents in accordance with given standards and provides it to users. Furthermore, ICEC developed its own filtering software, SafeNet 1.0, and is distributing it to public institutions, such as public libraries and schools. ICEC draws the structure of the SafeNet system as follows:

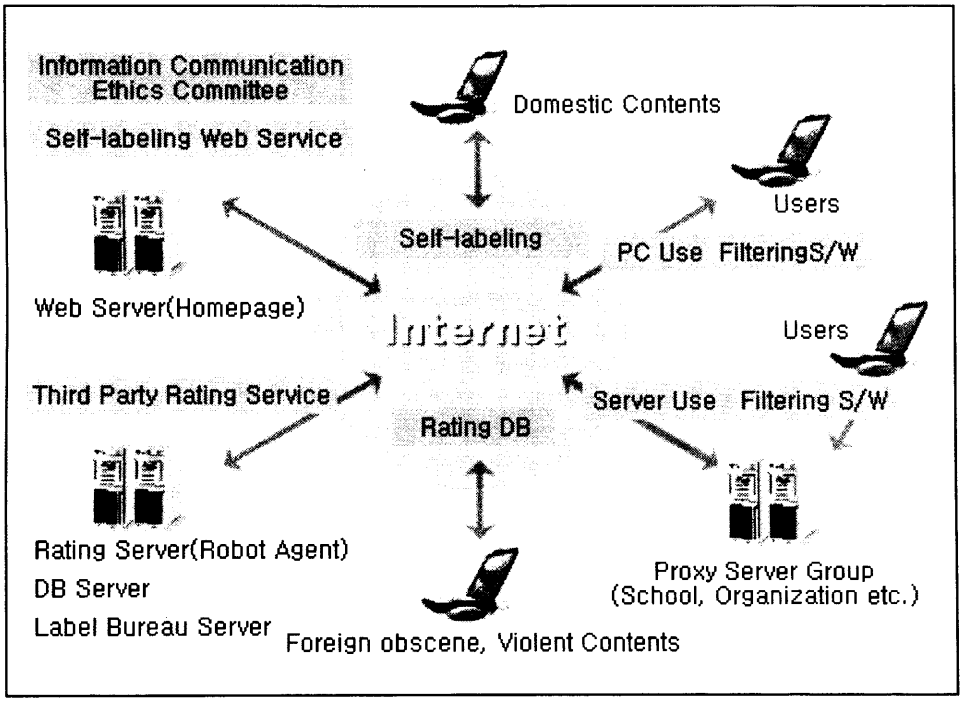

Fig. 7.1. Self-rating and third-party rating service of ICEC (Resource: SafeNet. Retrieved June 14, 2004, from http://www.safenet.ne.kr/english/intro/rating_system.html)

The SafeNet system does not allow other third-party's rating template, while ICEC provides third-party rating service itself. This is a significant difference between the SafeNet system and the ICRA system which provides multiple third-party rating templates as an important element of the rating system. In this sense, it can be said that the SafeNet system is an exclusive rating system of ICEC as compared to the ICRA system.

7.2.2. The Harmful-to-youth Material Indication System

In the indication system, there are three different methods to signify certain Websites as harmful-to-youth material: text, graphic logo and electronic indication. A material which is classified as harmful-to-youth information needs to clearly present the following sentence and graphic logo (MIC notification 2001-89) (Fig. 7.2).

> This information is harmful-to-youth material. According to *the Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.*, young people who are under 19 years old cannot use this information.

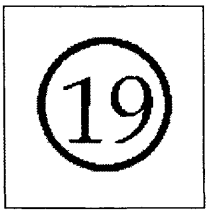

Fig. 7.2. The graphic logo of the harmful-to-youth material indication system.

These sentence and graphic logo should be displayed on a separated screen from a harmful-to-youth material. The separated screen should be a white background and full size, and the size of the sentence and logo should be more than one third of the full screen. In addition to these indications, a harmful-to-youth Website or Web page should provide an age verification device[18] (MIC notification 2001-89). A sample Web page (http://www.clubrich.com) which applies the harmful-to-youth material indication system is as follows (Fig. 7.3):

---

[18] In South Korea each individual is given an identification code, named JUMIN DEUNGROK BEONHO [Inhabitant Registration Number]. The persons who run a website can verify age of users and identify personal identity of users by checking users' Inhabitant Registration Number.

Fig. 7.3. A sample Web page with the harmful-to-youth material indication system

Another indication method is the controversial electronic indication system. ICEC has claimed that the harmful-to-youth material indication system is not a rating system. However, opponents recognise it as a compulsory Internet content rating system, since its electronic indication system is based on the PICS standard and grammar which most Internet content rating systems rely on. In my view, it is not a conventional Internet content rating system but as long as it is based on the PICS technical standard, it can be classified as a modified Internet content rating system. This system is compatible with Microsoft Internet Explorer and works just like any other rating system. In order to use this system, a user needs to download a RAT format file, "youth.rat"[19] and to

---

[19] The syntax of "youth.rat" file is as follows:

((PICS-version 1.1)
(rating-system "http://service.icec.or.kr/")
(rating-service "http://service.icec.or.kr/rating.html")
(name "harmful-to-youth medium material ")
(description "Under *Act on Promotion of Information and Communication Network*

install it on Microsoft Internet Explorer. This mechanism is just the same as the mechanisms of other rating systems, such as the RSACi system and the ICRA system.

The most significant difference between this system and other conventional Internet content rating systems is that the system provides only one designated value. It does not provide a variety of levels of information on the Internet. End-users are given only two descriptors: blocking the harmful-to-youth material or allowing it. The Microsoft Internet Explorer Content Advisor for the harmful-to-youth material indication system is shown below (Fig. 7.4).

Utilisation and Information Protection, etc. and its Enforcement Decree, a site which is indicated as harmful-to-youth medium material is blocked")

```
(category
 (transmit-as "y")
 (name "Do not allow access to harmful-to-youth medium material")
  (label
  (name "")
  (description "Do not allow access to harmful-to-youth medium material")
  (value 0) )
  (label
  (name "")
  (description "Allow access to harmful-to-youth medium material.")
  (value 1) )))
```

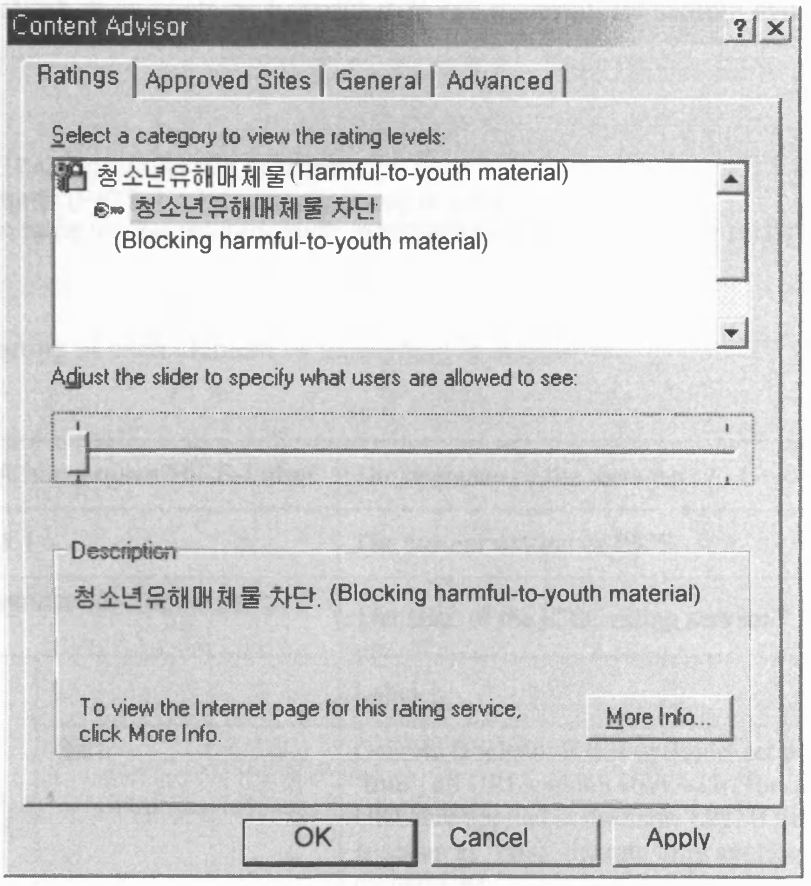

Fig. 7.4. Microsoft IE Content Advisor for the harmful-to-youth material indication system

According to the MIC notification No. 2001-89, harmful-to-youth information on the Internet should be indicated with the PICS technical standard which is recognisable by harmful-to-youth material filtering software. When a Website or directory contains harmful-to-youth material, its sample syntax is as follows. It looks very much the same as other conventional PICS-based rating systems' syntax:

```
<META http-equiv="PICS-label"
content='(PICS-1.1 http://service.icec.or.kr/rating.html
l gen true for "harmful-to-youth material indicated site or directory URL" r (y
1))'>
```

When a Web page contains harmful-to-youth material, its sample syntax is as follows:

```
<META http-equiv="PICS-label"
content='(PICS-1.1 http://service.icec.or.kr/rating.html
l gen false for "harmful-to-youth material indicated page URL" r (y 1))'>
```

The meaning of each element of this syntax is as follows:

<META http-equiv="PICS-Label"		The character of the meta tag
PICS-1.1		The current version of PICS
http://service.icec.or.kr/rating.html		The URL of the ICEC rating service
Labels [option]	L	Label
	Gen	Generic Boolean: if this option is set up as 'true', all URLs which start with 'for quoted URL' are applied at the same rate. If this option is set up as 'false' the rate only applies to the quoted URL
	for "URL"	URL which is rated
Ratings (<category><value>)		The designated value of harmful-to-youth materials is "y1"

Table 7.3. The syntax of the harmful-to-youth material indication system

In my view, the practical effects of this electronic indication system are doubtful. After I installed the youth.rat file on my Web browser, Microsoft Internet Explorer 6.0, I could not properly surf the Internet. There were virtually no Websites I could visit, unless I entered my administrator password or set to access all the Websites which are not rated using this indication system. For instance, I could not even access Kids Yahoo Korea, simply because it does not label itself with the system. Since the indication system is

applied only to Internet content which is deemed to be harmful, people who provide such child-friendly content are not obliged to rate their site with the indication system. Therefore, the most heavily trafficked Korean Websites, such as Yahoo Korea and DAUM,[20] are not within the scope of the indication system. However, this system is contradictory, because its success largely depends on the number of rated Websites as discussed in Chapter 5.5. For this reason it can be argued that the electronic indication method is impractical.

7.3. A Critique of ICEC Deliberation

South Korea had been ruled by military regimes from 1961 to 1992 (see Chapter 2.5). During the period, restraint of freedom of expression was rigorous. Although it has had the civilian form of government since 1992, freedom of expression is still restricted for various reasons from national security to obscenity. Since 1945 the country has been divided into South and North. The Cold War is still an ongoing issue in Korea. This unique political situation, coupled with strict moral standards (see Chapter 6.2.1.2), has constituted a ground of the government-centred regulatory policy of all media areas. The Internet is not an exception. As discussed in Chapter 6.3, information on the Internet has been subject to the rating system and post-deliberation of a governmental agency, ICEC.

In my view, most controversial issues concerning the Internet content rating system in South Korea are directly related to ICEC. First of all, it has been criticised for being a comprehensive governmental censorship body (S. Lee, 2001; Hwang, 2000). It has acted not only against harmful-to-youth content but

---

[20] According to Nielsen//NetRatings (2001b), by September 2001, a Korean portal site, DAUM (http://www.daum.net/) and Yahoo Korea (http://kr.yahoo.com) took 12th and 15th place respectively in terms of the biggest locally accessed Website.

also against controversial political content. For instance, in May 2000, ICEC terminated the Bak-Du Young Society's bulletin board that contained an article which applauded North Korea without first obtaining a court order (K. W. Cho, 2000). [21] On 27th May 2002 ICEC decided to suspend a Website, http://www.non-serviam.org, for two months because it discussed conscientious objection to military service and alternative forms of service (ICEC Document No. 2002-255). Three days later, at the request of ICEC the Korea Internet Data Centre (KIDC)[22] closed down all the services of the site's domain forwarding service company, Link Free,[23] for more than ten hours. Consequently, five thousand other Websites, which the Link Free serviced, also closed down. The service of the Link Free was recovered after it deleted non-serviam.org from its server and notified ICEC and the KIDC (Beom, 2002a; 2002b). The INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE (2002a) claimed that conscientious objection to military service is a widely recognised human right which has been clarified by the UN Human Rights Commission[24] and was critical of this incident for violating freedom of conscience which is articulated by Article 19 of the Constitution.

---

[21] As of October 2004, supporting North Korea is illegal in South Korea under *the National Security Law* which was enacted in 1948.

[22] KIDC is a subsidiary of Dacom, one of the biggest telecommunication companies in South Korea. Currently, KIDC is a leader in South Korean domestic Internet traffic (Retrieved October 12, 2002, from http://www.kidc.net).

[23] http://domain.linkfree.net/ (Retrieved April 4, 2005)

[24] In April 1998, the UN Commission on Human Rights adopted a resolution on Conscientious objection to military service (No. 1998/77). The resolution articulates, "it recognized the right of everyone to have conscientious objections to military service as a legitimate exercise of the right to freedom of thought, conscience and religion." The full text of the resolution is available on the UN High Commissioner for Human Rights Website at http://www.unhchr.ch/Huridocda/Huridoca.nsf/0/5bc5759a53f36ab380256671004b643a?Open document (Retrieved April 3, 2005).

During the five years, from 1997 to 2002, the cumulative number of deliberations on political matters was 3,607, including 130 deliberations on wild rumours, 134 deliberations on anti-nation issues and 3,343 deliberations on fraudulent election matters. In particular, in 1997, in 2000 and in 2002 when South Korea held a presidential election, a general election and a local election respectively, the numbers of deliberations on fraudulent election matters were 1,826, 703 and 812. In the year 2002, ICEC recorded 69 deliberations on anti-nation issues (see Table 7.4 and Appendix E). This figure clearly shows that ICEC constantly intervenes in political activities on the Internet.

Year / TDS*	Total	2002	2001	2000	1999	1998	1997
Wild rumours	130	5	30	13	34	34	6
Anti-nation	134	69	0	1	51	13	0
Fraudulent election	3,343	812	0	703	1	0	1,826

Table 7.4. The statistics of ICEC deliberations ***TDS**: Type of deliberated subject

Indeed, while many Internet self-regulatory bodies in Western countries, such as the Internet Watch Foundation, have focused on issues concerning child protection, ICEC has attempted to control all kinds of Internet issues. Its 24 deliberation categories and the number of deliberations in 2002 were as follows (Table 7.5):

Type of Violation	Number of deliberations	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights violation	5,649	2,618	9	61	2,398	150
Defamation / Privacy violation	116	21	17	4	0	0
Speculative spirit promotion / pyramid	422	115	58	22	27	8
Wild rumour	5	0	0	0	0	0
Anti-nation	69	3	0	3	0	0
Fraudulent election	812	0	0	0	0	0
Injustice advertisement	3	2	0	2	0	0
Obscenity / Violence text	990	531	315	85	108	23
Obscenity / Violence sound	5	3	3	0	0	0
Obscenity / Violence material sale	383	82	16	23	19	24
Obscenity / Violence material purchase	1	0	0	0	0	0
Obscenity / Violence material exchanging	68	49	5	43	1	0
Leading unhealthy meeting	531	350	155	136	28	31
Unhealthy chatting	659	599	10	559	28	2
Introducing a place of obscene material	4,531	773	349	289	122	13
Verbal violence	209	77	2	55	19	1
Prostitution	1	0	0	0	0	0
Obscene still image	8,792	3,362	1,708	56	2	1,596
Violence still image	59	21	9	3	0	9
Obscene movie	3,872	2,075	1,056	5	1	1,013
Violence movie	25	3	1	0	0	2
Obscene game	103	74	34	23	0	17
Violence game	58	0	0	0	0	0
Etc. / Out of classification	3,269	275	18	65	119	73
Non-deliberation subject	1,589	0	0	0	0	0
Total	32,221	11,033	3,765	1,434	2,872	2,962

Table 7.5. ICEC's deliberation categories and the number of deliberations in 2002

As Table 7.5 shows, ICEC took a significant number of deliberations which covered a broad area. In my view, ICEC's deliberations have a number of problems. Firstly, it is doubtful whether ICEC is able to provide expertise in these areas that include issues of copyright, privacy, politics and obscenity. Since 1998 ICEC has held an expert committee once a month. However, due to the amount of deliberations, the primary deliberation is carried out by administrative officers of the ICEC deliberation support team (D. Ahn, 1999). For instance, during the year 2002, the cumulative number of deliberations on obscene matters was 14,214 (see Table 7.5). Secondly, ICEC does not make any distinction between illegal and harmful content. As discussed in Chapter 2.4.1, in most countries the judiciary decides whether material is obscene or not. In most cases obscene material is subject to a criminal punishment, while indecency falls into an area of freedom of expression. However, regardless of whether material is "obscene" or perceive as "harmful," ICEC applies the same deliberation procedures to all categories. Thirdly, ICEC has never fully discussed these categories among the public, since it is able to set its deliberation categories itself under Article 16(2) of *the Enforcement Decree of Telecommunications Business Act.* Furthermore, the same Article allows the head of ICEC to bring up any matter for deliberation at will.

7.4. A Critique of ICEC Third-Party Rating

As regards the technical aspects, ICEC emphasises that the third-party rating system which uses compulsory proxing technology provides a more stable and efficient rating service because most of the harmful Internet content is hosted from abroad (see Fig. 7.1). However, it may raise a state censorship issue as third-party labelling can be done without any consent of information providers (see Chapter 5.2.1) so ICEC could confidentially label and filter a site without a due process. Since March 2000, ICEC has distributed a database, the so-

called "overseas unhealthy sites blocking list." The lack of clarity in standards and harsh marking procedure of the blocking list has raised many issues. The marking procedure of the blocking list is as follows. Firstly, an Artificial Intelligence robot gathers Websites which are linked to pornographic sites. Secondly, a few reviewers daily make hundreds of final decisions about rating categories and levels: nudity, sex, hate, demoralisation, violence, speculation and illegality. On 20th June 2001 the United Action Group's activists reviewed part of the blocking list (Ui, 2001). Many gay community sites were classified into the demoralisation category. Even the International Lesbian and Gay Association (http://www.ilga.org) which is one of the biggest and the most influential gay organisations worldwide, fell into the same category. Despite criticism from many organisations, no public verification or analysis has yet been made on this issue.

7.5. Conclusion

Under *the Communication Order Establishment Law* it is evident that the ICEC Internet rating system is in effect a governmental censoring device rather than a means of child protection on the Internet which was supposedly its original purpose. Firstly, ICEC is over-empowered; although ICEC is only an administrative organisation, it has effectively been given full judicial powers. Therefore, as discussed in the *Kim In-Kyu* case, it has often been criticised for not providing an appropriate due process. Secondly, the ICEC rating system deviates from the original aim of the Internet content rating system in terms of self-rating because ICEC can intervene against anyone's self-rating. Thirdly, in the name of third-party rating, ICEC virtually conducts upstream blacklist filtering. According to Kim Ki-Joong (2003), a legal counsel of the JINBO Network Centre, a backlist containing 145,198 Websites had been complied by June 2002. The ICEC third-part rating has been criticised for violating the rule

of clarity, since its rating list has not been fully available for review by concerned parties. Fourthly, the extent and object of the regulation is ambiguous. As discussed, ICEC has exercised its regulatory power over a wide range of Internet content and activities, from privacy violations to pornography, from illegal content to potentially harmful content. Although illegal content and harmful content are significantly different issues (see Chapter 2.4.1), ICEC deals with these two issues without distinction so that controversial content, which is indecent but lawful, is regulated in the way that obscene material is regulated. Thus, freedom of expression may be restricted.

As regards Internet content regulation, the government has the main responsibility for preventing users from accessing illegal content and taking part in illegal activities on the Internet. However, direct governmental intervention in the area of harmful content has been criticised for violating the rule against excessive restriction (14-1 KCC 616, 99Hun-Ma480, June 27, 2002). The reason why the Internet content rating system should not be conducted by governmental institutions is that the rating system is a solution for dealing with potentially harmful content. A mandated rating system may work as a tool of excessive governmental regulation on legal content which is deemed to be harmful. David Kerr, former chief executive of the Internet Watch Foundation (IWF), said in an e-mail interview:

> From IWF's experience in the UK and from close contacts with colleagues around the world, particularly in the US, Australia and the European Union member states, we are convinced that governments should take a "hands off" approach to labelling and filtering schemes.[25]

Of course, self-regulation cannot cover all the issues related to Internet content.

---

[25] The e-mail interview was conducted in July 2000.

It is only an option for preventing certain categories of people, in particular children, from accessing potentially harmful content. As discussed in Chapter 3, the EU has endorsed filtering and rating systems for this limited purpose. Illegal content is beyond the scope of these technical solutions.

Ironically, in South Korea the Internet content rating system, which was originally introduced as an alternative to legal regulation on the Internet through the CDA case (*ACLU v. Reno* 929 F. Supp. 824, 1996. see Chapter 2.6.1.1), is used by the government in order to rationalise its Internet content regulation. In this sense, the ICEC Internet rating system is a prime example of the ominous potential of Internet content rating systems. In the following chapter I will discuss in depth the impact of this governmental Internet content rating system on the actual Internet contents in South Korea.

CHAPTER 8

THE IMPACTS OF THE INTERNET CONTENT RATING SYSTEM ON THE ACTUAL INTERNET CONTENT IN SOUTH KOREA

8.1. Introduction

In the previous chapter, I discussed controversial Internet content regulations in South Korea. Furthermore, I explored ICEC's two different Internet content rating systems: the harmful-to-youth material indication system and the SafeNet Internet content rating system. As mentioned, it is noticeable that the Internet content rating system in South Korea is being directly driven by the government, while in many Western countries the Internet content rating systems have been established by the Internet industries and recognised as an important technical measure for dealing with harmful Internet content. Yet even these industry-based Internet content rating systems have been subject to severe criticisms (see Chapter 5.5 & 5.6). The governmental Internet content rating system in South Korea has raised many contentious issues. As discussed in Chapter 7, many civil rights organisations, such as the JINBO Network Centre, have perceived it as a means of governmental censorship. ICEC, the body of the governmental Internet content rating system, has intervened in all kinds of sites from political campaign sites to seemingly innocuous art gallery sites (see Chapter 7.3). Therefore, the impact of the Internet content rating system in South Korea is unique. In this chapter I shall discuss the impact of the governmental Internet content rating system on the actual Internet content in South Korea through two key case studies and my own survey.

8.2. Case Study I: EXZONE.COM

I will focus on two key cases, EXZONE.COM and iNOSCHOOL.NET, which have caught the media's attention and raised controversial issues in South Korean society for the last few years. My first case study concerns EXZONE.COM, the first gay Website in South Korea. Since South Korean society is permeated by a Confucian ethic that requires conservative standards

in public life, homosexuality is still highly controversial. Although the public's attitude towards these issues has been steadily changing, partly because of the rapid Westernisation of South Korean society and partly because of many gay and lesbian activists' campaigning efforts, prejudice against homosexuality is still widespread and deeply ingrained in society.[1] In December 2000, a famous TV show presenter, Hong Suk-Chun, was the first celebrity in South Korea to 'come out.' His coming-out resulted in a fierce debate on homosexuality (Shin-Yun, 2000). After the incident, he was dismissed from his show and since then no broadcasting station has hired him.

In this sense, the advent of the first gay Web community, EXZONE, has played an important role, since it has successfully established a public sphere where people for the first time can freely discuss, share and exchange their opinions and experiences about gay issues. Nevertheless, it became the first case of a site that was forced to close down under the so-called harmful-to-youth medium material indication system. It clearly shows how the South Korean government's Internet content rating system can silence the voice of minority groups on the Internet. These are the reasons why I have chosen this as my first case study.

EXZONE was started by a man who is nicknamed Jung-Chun (literally, queen: he does not want to make his real name public) on 6th June 1997. At the

[1] Until the early 1990s, the South Korean gay/lesbian community remained strictly hidden from the public. It merely existed in few ghettos of large cities, such as Nakwondong in Seoul. In November 1993, the first gay/lesbian rights activities group, CHODONGHOE was established. Later, it is divided into the Korean Gay Men's Coalition, CHINGUSAI [Between Friends] and the Korean Female Sexual Minorities' Rights Group, KIRI KIRI [Group by group]. (Kiri Kiri, 2004).

beginning EXZONE used Chollian's[2] sub-domain and Web space. Since the 6th March 1999 it has used the domain, EXZONE.COM (EXZONE, 2001b).

According to Jang Yo-kyong of the JINBO Network Centre (Jang, 2002), the Webmaster Jung-Chun has retained the anonymity of all users in order to make an independent cyber community for people who are alienated and discriminated because of their sexual orientation. This Website was also famous for its strict "Netiquette." From the beginning the site clearly displayed an administrative policy on its bulletin board. Any inappropriate articles were immediately deleted by the site's management group. EXZONE (2001b) did not allow articles which contain any swearwords, obscene expressions, detailed personal information except e-mail address, for instance real addresses and telephone numbers or commercial advertisements. Articles which infringed someone's privacy or defamed someone's character were deleted. Articles that violated any other laws were also not allowed.

Although many users have complained about the strict policy — it was said that the policy is oppressive and even violates free speech rights — EXZONE has always made an effort to strictly adhere to its policy. The issue of access to EXZONE by people under 18 years old caused a heated argument between the manager group and some users. They reached an agreement even on this issue throughout a users' discussion in August 1999. After that EXZONE did not allow access by people under 18 years old (Shin-Yun, 2001a). The Webmaster Jung-Chun stated that:

> From the technical point of view, it is impossible to completely block under 18 years old people's every single access to EXZONE. It is also

[2] Chollian, South Korea's first on-line service, was introduced in 1985.

> impracticable to block indiscreet adults who may harm minors. Although we cannot block their access, we refuse to abandon our policy standards (Jung-Chun, 1999).

As a result of these efforts the site grew into a very moderate cyber gay community. Furthermore, it became the largest one in South Korea. The International Gay and Lesbian Human Rights Commission's (IGLHRC) Website[3] linked to EXZONE.

However, on 25th August 2000 — almost three years after the site launched — ICEC classified EXZONE as a harmful-to-youth medium. Ironically, the reason for ICEC's classification was obscenity. A month later CHEONGSONYEON BOHO WIWONHOE [Commission on Youth Protection] (CYP)[4] issued an official notification (No. 2000-31) of the ICEC's deliberation on EXZONE (M. Lee, 2004, p. 23). The formal document of the notification is in Appendix F.

However, EXZONE was not informed about the decision and remained unaware of it for a year. Surprisingly, neither ICEC nor CYP cautioned EXZONE before they made the final decision (S. Lee, 2002). Even after issuing the notification, they did not inform EXZONE that it was named as harmful-to-youth medium, although this matter was directly related to the EXZONE owner's legal responsibility under Article 42 of *the Act on*

---

[3] IGLHRC is a US-based non-profit, non-governmental organisation (NGO). The mission of the International Gay and Lesbian Human Rights Commission (IGLHRC) is to secure the full enjoyment of the human rights of all people and communities subject to discrimination or abuse on the basis of sexual orientation or expression, gender identity or expression and/or HIV status (Resource: IGLHRC. Retrieved October 11,2002, from http://www.iglhrc.org)

[4] The Commission on Youth Protection was established in July 1997. It is the administrative organisation affiliated with the Prime Minister's Office which carries out various policies and business designed to protect youth from harmful environments (Resource: CYP. Retrieved August 1, 2002, from http://www.youth.go.kr)

Promotion of Information and Communication Network Utilisation and Information Protection, etc. (see Chapter 7.1.3) and Article 14 of *the Juvenile Protection Act.*[5] The EXZONE's Webmaster, Jung-Chun, found it out by accident when he joined the anti-Internet censorship campaign in July 2001. After that he immediately made a formal objection and urged two organisations, ICEC and CYP, to repeal the decision (S. Lee, 2002).

Both ICEC and CYP delayed their reply without giving an adequate excuse. Subsequently, the situation deteriorated. On 30th July 2001 another gay Website, IVANCITY, was closed by its Web hosting company just after ICEC posted an official letter to the Korea Internet Data Centre (KIDC).[6] KIDC then requested the hosting company to terminate its service for IVANCITY (Shin-Yun, 2001b). On the same day, many Korean gay and lesbian Websites went on a one-day strike protesting against the harmful-to-youth material indication system (see Chapter 7.2.2) which classifies homosexuality in the demoralisation category and *the Juvenile Protection Act* which defines homosexuality as an abnormal sexuality similar to sadism and masochism (EXZONE, 2001a).[7] On 31st July 2001 fifteen gay and lesbian organisations, including EXZONE, jointly

---

[5] Article 14 (Obligation of Indications) of *the Juvenile Protection Act*

> (1) Any media materials harmful to juveniles shall carry indications that they are harmful to juveniles (hereinafter referred to as the "juvenile harmful indications").

[6] see Chapter 7: Footnote 21.

[7] Article 7 of *the Juvenile Protection Act Enforcement Decree* states the deliberation standard of harmful-to-youth media in an appended chart. In particular, Article 7. 2(Da) defines homosexuality as an abnormal sexuality.

> Article 7 (Harmful-to-Juvenile Medium Deliberation Criteria)
>
> 2. Individual Deliberation Standard
> Da. Describing bestiality or bolstering sexual relationships which are not allowed by a social common notion, such as abnormal sexuality-including group sex, incest, ***homosexuality***, sadism, and masochism, prostitution and the others

launched the Lesbian and Gay Alliance Against Discrimination in Korea (LGAAD Korea) (Soh, 2001). On 26th August the International Gay and Lesbian Human Rights Commission's (IGLHRC) posted an e-mail to call for urgent letters of protest against the South Korean government's discriminatory Internet content rating system to its members all over the world. The e-mail stated as follows:

> [ICEC] has classified homosexuality in the category of "obscenity and perversion" in its "criteria for indecent Internet site" and called for the blockage of all gay and lesbian Internet sites in Korea. [...] These actions violate the right to freedom of expression enshrined in Article 19 of the International Covenant on Civil and Political Rights[8] [...] which Korea is a signatory. Articles 2 and 26 of the International Covenant on Civil and Political Rights[9] recognise that all persons are equal before the law and are entitled to protection from discrimination on any ground, including race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. The United Nations Human Rights Committee has held this definition to include sexual orientation as a status protected from discrimination (IGLHRC, 2001).

---

[8] see Chapter 2.1.

[9] The full text of Article 2(1) and Article 26 of the International Covenant on Civil and Political Rights are as follows:

> Article 2(1)
> 1. Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
>
> Article 26
> All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

On 10th October ICEC finally rejected EXZONE's appeal. On 9th November EXZONE received a letter from ICEC that stated as follows:

> According to *the Act on Promotion of Utilisation of Information and Communication Network and Information Protection*, [Your site] has an obligation to mark itself as a harmful-to-youth medium using text, graphic, and electronic methods together. If you do not fulfill it, you can be penalised with a fine of 10 million KRW (about 5,400 GBP) or two years' imprisonment. Please, take action on it soon; otherwise you may unnecessarily invoke a sanction (EXZONE, 2001c).

On 9th November EXZONE closed itself down. The Webmaster turned the EXZONE home page black and left a message as follows:

> I disagree with the authorities that I have infringed the law. I simply do not know why I have received a letter threatening me with a fine and imprisonment. There is no objective evidence that EXZONE is harmful to Korean youth. I have asked ICEC to inform me precisely what content is deemed to be obscene, but ICEC has failed to produce an answer. I do not need the official letter which forces me to comply with ICEC's Internet content rating system. [...] I will close down my EXZONE rather than agree to labelling it an obscene medium (EXZONE, 2001c).

In January 2002 EXZONE filed an administrative lawsuit for annulling the harmful-to-youth material notification to EXZONE (S. Lee, 2002). The plaintiff claimed that in EXZONE's case the criterion of ICEC's harmful-to-youth medium deliberation is based on Article 7(2)(Da) of *the Juvenile Protection Act Enforcement Order*,[10] in particular bolstering homosexuality, however, this deliberation criterion does not come under the mother law,

[10] see Chapter 8: Footnote 6.

Article 10(1) of *the Juvenile Protection Act*[11] at all. Therefore, Article 7(2)(Da) of *the Juvenile Protection Act Enforcement Order* is void. For the same reason ICEC's deliberation and CYP's notification proceeding on EXZONE is invalid. Furthermore, ICEC defined EXZONE as a harmful-to-youth medium by reason of not only bolstering homosexuality, but also some obscene articles which were posted to EXZONE's bulletin board. This decision ignored the fact that no Webmaster is able to simultaneously manage all articles on a bulletin board. Even if there were a few obscene articles on the bulletin board, it cannot be said that the whole bulletin board was obscene (LGAAD Korea, 2002).

However, EXZONE lost the case in August 2002. Judge Han Gi-Taek of Seoul HAENGJEONG BEOPWON [Administrative Court] dismissed all the plaintiff's

---

[11] The full text of Article 10 of *the Juvenile Protection Act* is as follows:

> Article 10 of *the Juvenile Protection Act* (Criteria for Deliberation of Media Materials Harmful to Juveniles)
>
> (1) In performing the deliberation in accordance with the provisions of Article 8, the Commission on Youth Protection and each deliberative organisation shall identify the media material in question as harmful to juveniles, in the case where the media materials in question fall under any of the following subparagraphs:
>
> 1. Voluptuous or obscene materials which may stimulate sexual desire in juveniles;
> 2. Materials which may cause violence and brutality of juveniles or incite them to commit a crime;
> 3. Materials which may encourage or justify violence including rape and the abuse of drugs;
> 4. Materials which are anti-social and non-ethical and that may hamper the cultivation of fine character and civic consciousness in juveniles; and
> 5. Materials which are feared to affect harmfully the mental and physical health of juveniles.
>
> (2) In specifically applying the criteria referred to in paragraph (1), the generally accepted ideas of society shall be based, and literary, artistic, educational, medical and scientific aspects as well as characteristics of the media materials concerned shall be taken into account.
>
> (3) Necessary matters concerning the specific criteria for deliberating whether or not any media materials are harmful to juveniles and its application shall be prescribed by the Presidential Decree.

claims (Judgment of August 14, 2002, 2002GU-HAP1519).[12] Although the Judge recognised that ICEC and CYP's decisions on the EXZONE case were problematic, he rejected the plaintiff's request, because the plaintiff did not adhere to a deadline regarding the timing of the legal proceedings (M. Lee, 2004, pp.23-25). According to *the Juvenile Protection Act*, "Any person, who is dissatisfied with a disposition taken under this Act, may raise an objection to an administrative agency which has taken the disposition, citing the reasons thereof, within 60 days from the day he is notified of the disposition." (Article 39) and "Any person, who intends to institute a litigation against a disposition taken under this Act, shall institute the litigation within 90 days from the day he is notified of the disposition." (Article 40). EXZONE entered an appeal to a higher court. However, in December 2003 the appellate court affirmed the judgment of the lower court (Judgment of December 16, 2003, Seoul GODEUNG BEOPWON [High Court], 2002NU14418).[13] In the same month EXZONE appealed again to the Supreme Court (EXZONE, 2004). The case is in progress as of April 2005.

In fact, EXZONE was not closed down by ICEC. It closed itself down to protest against the harmful-to-youth material indication system. What would have happened, if EXZONE had not closed itself down? It might have been either sentenced to imprisonment[14] or lumped together with explicit pornography Websites. If EXZONE had rated itself under the indication system, it would have had a front page which declared its harmfulness. Every one of its

---

[12] The full text of the judgment is available in Korean on archived LGAAD Korea Website at http://outpridekorea.com/ttboard/ttboard.cgi?bname=NOTICE (Retrieved April 5, 2005).

[13] The full text of the judgment is available in Korean on archived EXZONE Website at http://exzone.com/html/ (Retrieved April 5, 2005)

[14] see Chapter 7.1.3.2.

users would have passed through an age verification system.[15] There would have been a significant difference in terms of accessibility and visibility. Furthermore, regardless of whether EXZONE would have rated itself or not, ICEC could label EXZONE as harmful-to-youth material through its third-rating system. Therefore, access to EXZONE at public Internet access points, such as PC-cafés, would have been restricted due to obligatorily installed filtering software. Ironically, the indication system has less impact on adult content sites. Apart from illegal obscene sites, most legitimate commercial adult content sites have provided adult verification devices for commercial purposes, even before the indication system was introduced. In most cases, explicit adult content is accessed in privacy rather than at public places.

As mentioned in the previous chapter, the theory of the Internet content rating system which is based on the PICS specifications empowers Internet users to control their own access to Internet content, and would reduce the risk of government censorship (see Chapter 5.4). On the contrary, as discussed through the above study, in South Korea the Internet content rating system rather raises censorship issues. Indeed, it works as a powerful governmental Internet content regulating measure. Consequently, the Internet content rating system has faced tough challenges. As discussed in the previous chapter, this may remain as a critical obstacle to an Internet content self-regulating system. Such a system cannot be successful without the general public's co-operation, because it relies largely on uncompensated effort by Internet users (see Chapter 5.5).

---

[15] There are three different methods to indicate sites as harmful-to-youth material: text, graphic logo and electronic indication (see Chapter 7.2.2).

8.3. Case Study II: iNOSCHOOL

The second case study is iNOSCHOOL, a teenagers' Internet community which discusses alternative schooling. As with the EXZONE example, this case shows how the government-centred Internet content regulation has restricted minorities' rights.

South Korean society is obsessed with academic qualifications. It places excessive value on academic qualifications as a valid measure of a person's ability (Jin, 2003, pp. 71-72). Competition for entering prestige universities is extremely fierce. As a result, education takes precedence over most other public issues. As of the mid 1990s, the ratio of students going on to colleges and universities had already reached about 50 percent (J. Han, 1996, p. 176).[16] However, these social trends have resulted in the public education and schooling system focusing almost exclusively on preparing students for the university entrance examination. Not surprisingly therefore, the South Korea education and schooling system is still rather authoritarian and is characterised by a cramming ethic as compared to an educational ethic that encourages discussion and student autonomy.

As early as the early 1980s this kind of issue began to be discussed. Since the early 1990s it has become evident that schools are no longer successfully fulfilling their purpose and 'school failure' has become a serious social issue (Jin K. Kim, 1997). This situation has not been resolved; the school system is still being attacked from many different quarters. As a result, alternative education and schooling systems have been discussed not only by many education experts but also by many students through a number of cyber

[16] As of the mid 1990s almost all primary school students went on to middle schools. 89 percent of middle school students entered high schools (Han, 1996, p. 176).

communities. Under the existing authoritarian schooling system, it is very difficult for teenage students to openly discuss and criticise the system they belong to. Therefore cyberspace, as represented by the Web, is the ideal medium that enables them easily to establish their own community and to voice their opinions freely.[17] iNOSCHOOL was one of these cyber public spheres. Unfortunately, the hands of governmental Internet regulation intervened even in this small cyber community. It became the first case of a blockage of teenagers' voice on the Internet. As such it represents an important instance of government intervention which is why I have chosen this as my second case study.

A teenagers' Internet community, iNOSCHOOL was officially launched in November 2000. Originally, it was a personal Website of a 15 years old boy, Kim Jin-Hyuk, who voluntarily left his middle school. A few months later, however, it became a small cyber community, so-called 'No School Student.' Five months after the original Website opened, this cyber community made a new start with its own domain name, iNOSCHOOL.NET (Jin H. Kim, 2001).

iNOSCHOOL is an Internet community not only for teenagers who drop out of school, but also teenagers who attend school. iNOSCHOOL has established a unique cyber public sphere where teenagers freely share and exchange their worries and information. On its bulletin board they make their voices heard on school and educational issues, but any article which contains abusive language is immediately deleted by the Webmaster with the exception of articles which

[17] It is an interesting fact that teenagers are the most enthusiastic Internet user group in South Korea. According to a survey from NCA (2002, p. 56), as of December 2001, the number of Internet users who belong to the age group from 7 to 19 amounted to 8.43 million which represented about 35 percent of the total Internet users in South Korea. This is the largest age group followed by twenties, thirties, and forties with 29 percent, 22.4 percent, and 10.5 percent respectively.

inevitably use swear words in order to describe and discuss his or her own experiences at school (IDOO, 2002b). This strict administrative policy is quite similar to EXZONE. They did not blindly criticise school but discuss and search for solutions for improving schools. Moreover, they have made efforts to change social prejudices against teenagers who do not belong to the school education system through their newsletter and off-line meetings. iNOSCHOOL can be said to be a moderate cyber community (Hong, 2003).

However, in June 2001 iNOSCHOOL was forcedly shut down by ICEC (Jae S. Kim, 2001). The reasons given by ICEC for its action were as follows:

> This site aims at radically criticising school. Furthermore, it encourages juveniles to leave school and home through positive expressions about these kinds of behaviour on its bulletin board. Therefore, its bad influence is a matter of grave concern. We therefore deem this site as falling into the 'unhealthy information category' as defined by Article 16(3) of *the Telecommunication Business Act Enforcement Decree* (IDOO, 2002a).

The majority of ICEC deliberation committee members decided to issue an order that the iNOSCHOOL's Web service company should terminate the Website under Article 16.4(3) of *the Telecommunication Business Act Enforcement Decree* which rules revision orders.[18]

---

[18] The full text of Article 16.4(3) of *the Telecommunication Business Act Enforcement Decree* (Revision Order) as follows:

> (1) If a certain information fall under improper communication which is defined by Article 16 on the basis of the deliberation which defined by Article 16(3), under Article 53.2(4)(2) the committee can require a telecommunication company which hosts the improper information to comply with each Article below.
>
> 1. Warning to user
> 2. Deletion of information
> 3. Use cancellation or use suspension of a user who practices improper communication which is defined by Article 16

Usually, individuals or small non-profit organisations manage their Website using ISPs' Web servers, while most big companies and organisations run their own Web facilities at high costs. If an ISP suspends its service for a user who runs his or her own Website using the ISP's Web server, no Internet user can access the Website. Therefore, ICEC's order which forces ISPs to one-sidedly cancel a Web service contract without a user's consent means the end of the user's Website.

Just like the EXZONE case, ICEC did not give iNOSCHOOL a proper warning. On 8th June 2001 iNOSCHOOL's Webmaster received a telephone call from ICEC. On the very same day the site was shut down. Hundreds of teenagers posted protest e-mails to ICEC and the South Korean Presidential Mansion's Websites (G. M. Lee, 2001). iNOSCHOOL applied to ICEC for the second deliberation. INOSCHOOL's Webmaster argued that:

> In a democratic society all citizens should enjoy freedom of speech and the press, and of assembly and association. All groups may freely express their ideas and opinions. iNOSCHOOL is a public sphere where people speak and discuss all aspects of schooling (IDOO, 2002a).

ICEC rejected iNOSCHOOL's appeal on 18th July 2001 (IDOO, 2002c). Despite these incidents, iNOSCHOOL returned to normal. Since iNOSCHOOL moved all its Web contents to the JINBO Network Centre's Web server in July

---

(2) If a telecommunication company takes a correction requirement under Article 1, it should report a result of the proceeding to the committee.

(3) The committee can propose to the Ministry of Information and Communication (MIC) Minister that the Minister should give refusal, suspension, and restriction order against "improper communications" under Article 53, if the telecommunication company do not comply with the correction requirement.

2001, ICEC has taken no action on iNOSCHOOL (Kim & Lee, 2001). In this case, the only way to block out iNOSCHOOL is a blockage of its new Web server which hosts many other civil organisations' Websites. This action may result in a massive blockage of many legitimate Websites. In my view, it seems that ICEC does not want to provoke the hostility of hundreds of civil organisations. A reporter called the JINBO Network Centre's server "cyber Myeongdong Sungdang [Myeongdong Cathedral]" which was famous for being a sanctuary of pro-democracy activists in the 1980s (C. Ahn, 2001). To sum up, the iNOSCHOOL case revealed both the lack of consistency of ICEC's deliberation and the inefficiency of its Internet content regulating system.

8.4. Rating and Removal Orders

Notably, ICEC took different regulatory actions to EXZONE and iNOSCHOOL respectively. While EXZONE was forced to rate itself, iNOSCHOOL was shut down without any notice. In a sense, the iNOSCHOOL case shows ICEC's worst regulatory practice. ICEC did not force iNOSCHOOL either to rate itself or to revise its content, but it expelled the whole site from the Internet. ICEC's incompetence was shown when iNOSCHOOL moved to another Web sever and ICEC did not take any further action. ICEC could not provide justification of its regulatory practice and the incident showed that the Internet environment provides a way to incapacitate such removal orders. Even if ICEC entirely blocks out a site, a number of replicas of the blocked site can easily be set up.

As discussed above, the Internet has enabled social minorities to speak out, to voice their concerns and to build their own communities in a cheap and convenient manner. The Internet has provided them with great opportunities

which they previously never had. However, the South Korean government's Internet content regulation, which was intended to deal with illegal and harmful-to-youth Internet content, interrupts the voices of vulnerable and powerless social minorities. Indeed, it strongly impacts on the online communities of social and sexual minorities. These online communities have become the first victims of ICEC's inconsistent deliberation system and its irrational notification procedure.

While South Korean society has rapidly Westernised, the government's Internet content deliberation system seems to lag behind. It is clear that South Korean Internet content regulators and a number of netizens who have spontaneously participated in those Internet communities have quite different viewpoints concerning issues of Internet content regulation. It can be said that the South Korean government's Internet content regulation, including the mandatory Internet content rating and deliberation systems, has had a derogatory effect on South Korean Internet communities, because it has been imprecise and unpredictable. A study by the JEONGBO TONGSIN JEONGCHAEK YEONGUWON [Korea Information Strategy Development Institute] criticises ICEC for the inflexible manner in which it has practised its regulatory power. It points out, through a number of cases, such as Kim In-kyu, iNOSCHOOL and Non-serviam.org, that ICEC did not provide a predictable regulatory system (Kim, Jeong, Lee & Oh, 2001, pp. 100-103). Through these cases, civil rights organisations, such as JINBO Network Centre, have continued activities to protest against the government-centred regulatory system and demanded amendment to the law related to Internet content regulation (K, Kim, 2003). In this context, the above two cases have worked as the catalyst to reform Internet content regulation in South Korea.

8.5. Questionnaire Analysis

8.5.1. Introduction

This questionnaire was designed to survey the impact of the Internet content rating system on actual Internet content in South Korea. In particular, the survey will focus on the harmful-to-youth medium material indication system, although it is still disputed whether this system is in fact an Internet content rating system. As mentioned in the previous chapter, this is not a conventional Internet content rating system, but a modified Internet content rating system. However, the government argues that this system is only an electronic version of the existing harmful-to-youth medium material indication system which has been applied to traditional media, such as newspapers, books and magazines and gained public approval (MIC notification 2001-89). Furthermore, it is the only mandatory Internet content rating system that has generated so much controversy and debate. Therefore this survey has been created with two separate sections with questions pertaining both to the conventional Internet content rating system and to the harmful-to-youth medium material indication system. The questionnaire consists of four sections: general information, the Internet content rating system, the harmful-to-youth medium material indication system and rating and labelling with three, seven, five and ten questions respectively. The total number of questions is 25. All questions are pre-coded but some questions also provide open-ended choices.

The population for this study is Korean Websites. The sample was selected from among Web experts who work for Korean Websites and the sample was drawn from the on-line edition of the Google Korean Website Directory (as of December 2002) which has 17 categories with 317 sub-categories. The first four links of each sub-category, 799 links in total, were selected (see the full

sample list in Appendix H). From this number, 140 links which were broken or did not provide any e-mail address were excluded. This resulted in a set of 659 sample Websites. The questionnaire was sent to the individuals in charge of these sample Websites, such as Webmasters, via e-mail. Reminders were sent four times every seven days, along with a repeat posting of the original questionnaire. The final response rate was 9.56 percent with 63 usable responses. This survey was conducted over a five week period, between 6th January 2003 and 10th February 2003.

8.5.2. Section I: General Information

The first three questions of the questionnaire asked respondents about their occupation, Website classification and target audience. The key findings of these questions are as follows:

Q1. Please state your occupation or job title.

As initially intended, this questionnaire was conducted on people who are in charge of managing Websites, not ordinary Korean Web users. Almost 90 percent of all respondents, 56 out of 63 respondents, have an Internet-related job title, ranging from Webmaster to e-businessman.

Q2. How would you class the Website which you own or work for? Tick or complete all relevant options.

The largest number of respondents classified their Websites into the *Business* category with 26 percent, followed by *Organisation* with 22 percent. Since this sample was drawn from the Google Korean Website Directory, it was to be expected that most of the sample sites would belong to commercial companies

or non-profit making organisations, rather than individuals. This result confirms the forecast.

Q3. What is the age group of your site's target audience? Tick or complete all relevant options.

The dominant age group of the sample sites' target audience is *adults* with 71 percent, followed by *teenagers* with 20 percent. However, this does not necessarily mean that these sites provide explicit adult information. In reality, a site's real audience can differ from its initial target audience. In this sense, this figure represents the sample sites' estimated target audience, rather than their actual audience.

8.5.3. Section II: The Internet Content Rating System

The second section of the questionnaire consists of seven questions that ask respondents about their knowledge and opinions of the Internet content rating system. The results are as follows:

Q4. Have you heard about the Internet content rating system? (*If YES, please answer all questions from Q5 to Q10. If NO, please go to Q11*)

	%	No.	
Yes	**75**	**47**	
No	25	16	
Not-answered	0	0	
Total		63	

Table 8.1. The result of the questionnaire [Q4]

A quarter of respondents who take the responsibility for managing Websites had no knowledge of the Internet content rating system. Presumably a much

lower percentage of ordinary Web users would answer "yes" to this question. The Internet content rating system is based on users' voluntary participation. In order for the system to be effective, the number of rated Websites should reach a critical mass compared to the total number of Websites. In this sense, gaining a wide range of public consent and popularity is one of the prime issues for developing the Internet content rating system. However, the above result shows us that the Internet content rating system in South Korea is still not sufficiently well-known and therefore it is underused.

Q5. If YES, tick or complete all relevant boxes.

	%	No.	
ESRBi[19]	5	6	
ICRA system	13	15	
MedCERTAIN[20]	2	2	
RSACi system	10	12	
SafeNet system	**20**	**24**	
	11	13	
SafetyOnline	16	19	
None	12	15	
Not-answered	12	15	
Total		121	

Table 8.2. The result of the questionnaire [Q5]

[19] The Entertainment Software Rating Board (ESRB) is a self-regulatory body established in 1994 by the Interactive Digital Software Association, US. It has developed a standardised rating system for video game, computer game and Internet game software. The ESRBi system is the online rating unit of ESRB. It provides age-based ratings for Websites.

[20] MedCERTAIN is an abbreviation for "MedPICS Certification and Rating of Trustworthy and Assessed Health Information on the Net." It is a project to establish an international trustmark for health information. It has been funded by the European Union under *the Action Plan for Safer Use of the Internet.*

ICEC's SafeNet system takes first place with 20 percent of the responses. Among seven listed systems, this is the only system operating in Korean — SafetyOnline is serviced in Japanese and the other five systems are serviced in English. The second most well-known system is IAJapan's Safety Online with 16 percent, followed by the ICRA system, the SafeSurf system, and the RSACi system. It could be posited that the reason for the Safety Online system taking the second place is largely based on confusion between two systems which have very similar names; the Safety Online system and the SafeNet system. The Safety Online system has not been officially introduced in South Korea, nor does it operate in Korean. The ICRA system which is the most well-known Internet content rating system in Europe takes third place. In 2002 the Korean Internet Self-regulation Forum signed a license contract of the ICRA system with ICRA. It does not yet service the ICRA system in Korean. In this sense, it could be claimed that the result of this question does not directly represent the respondents' practical preference or frequency in use of the rating system.

Number of specified systems	Number of respondents	
None	**15**	
1	9	
2	8	
3	5	
4	6	
5	4	
6	0	
7	1	
Not-answered	**15**	
Total	63	

Table 8.3. The result of the questionnaire [Q5a]

33 respondents out of 63 respondents named at least one system, while 15 respondents said "none" and the same number of respondents did not reply to this question.[21] Only one respondent answered that he/she knows all the seven listed systems. Nine respondents said that they know just one out of the seven listed systems (see Table 8.3). Furthermore, of the 47 respondents who answered that they know of the Internet content rating system in question Q4, about 30 percent were unable to name any specific system.

Q6. How confident are you in using the Internet content rating system?

	%	No.	
Very confident	14	9	
Fairly confident	22	14	
Not at all confident	**42**	**26**	
Not-answered	22	14	
Total		63	

Table 8.4. The result of the questionnaire [Q6]

Significantly, 42 percent of respondents answered that they are *not at all confident* in using the Internet content rating system, while only 14 percent were *very confident* about using the system. Of 26 respondents who answered "not at all confident" 14 respondents do not specify any rating system in their answers to question Q5. Seven and three respondents specify one and two systems respectively. One respondent named three systems. In this sense, "not at all confident" can be interpreted as meaning that respondents merely know the name of a system and do not have any detailed knowledge. As with the

[21] It was stipulated that a respondent could answer questions from Q5 to Q10, if he or she answered "yes" to question Q4. However, two of 16 respondents who answered "no" to question Q4 ignored this instruction; one answered all questions from Q5 to Q10, and another replied to questions Q6 to Q10.

previous question, the results of this figure show that almost 65 percent of respondents lack proper knowledge of the Internet content rating system. In my view, it does not mean that respondents' general technical knowledge is low. It simply means that they do not have much interest in the Internet content rating system and the system does not have the intended effect on their Internet activities. As discussed in Chapter 5, people's low level of participation results in the rating system having little practical force and then this reproduces people's poor involvement on an enlarged scale. The Internet content rating system in South Korea is not an exception.

Q7. The Internet content rating system is an efficient technical solution to protect minors from harmful information on the Internet. Do you agree?

	%.	No.	
Strongly agree	8	5	
Agree	**24**	**15**	
Disagree	21	13	
Strongly disagree	3	2	
Unsure / Don't know	22	14	
Not-answered	22	14	
Total		63	

Table 8.5. The result of the questionnaire [Q7]

In this question the respondents' answers are evenly split into three major groups; "agree," "disagree" and "unsure/don't know." In my view, the responses to this question confirm that it is still highly controversial whether the Internet content rating system is an efficient technical solution to protect minors from harmful information on the Internet. While 32 percent of respondents display a positive attitude to the rating system as an efficient technical solution for dealing with harmful information on the Internet, almost

half of them are unsure. Thus, it can be said that respondents doubt the rating system's efficiency and its original purpose as a neutral technical solution.

Q8. The Internet content rating system may violate freedom of expression on the Internet. Do you agree?

	%.	No.	
Strongly agree	11	7	
Agree	14	9	
Disagree	**29**	**18**	
Strongly disagree	8	5	
Unsure / Don't know	16	10	
Not-answered	22	14	
Total		63	

Table 8.6. The result of the questionnaire [Q8]

It is significant that almost 40 percent of the respondents objected to the idea that the Internet content rating system may violate freedom of expression on the Internet, despite much controversy and dispute relating to the governmental Internet content rating system. However, it is still significant that a quarter of the respondents felt that the Internet content rating system could have a negative effect on freedom of expression on the Internet.

The public's attitude to sexual information is still conservative, mainly because South Korean society is permeated by a conservative Confucian influence which requires high standards in public life (see Chapter 6.2.1.2). Issues of harmful information on the Internet, in particular pornographic contents, have become a serious social concern. In this sense, the current social concern seems to slightly outweigh the right to free speech. For this reason the South Korean government has claimed that some kind of regulatory solution on the Internet is

urgently needed and finally introduced the mandatory rating system.

Q9. Do you agree that a governmental institution should operate the Internet content rating system?

	%	No.	
Yes	8	5	
No	**57**	**36**	
Don't know	13	8	
Not-answered	22	14	
Total		63	

Table 8.7. The result of the questionnaire [Q9]

Notably, 57 percent of the respondents opposed the idea of a governmental institution operating the Internet content rating system, while a mere 8 percent supported it. Although the responses to the previous two questions, Q7 and Q8, show that the respondents' attitudes to the Internet content rating system are uncertain, their attitude to a governmental institution's Internet content rating system is very clear.

In other words, while one-third of respondents support the system as an efficient solution to protect minors from harmful information on the Internet and deny the system's negative effect on freedom of expression, only a handful of respondents agree with the governmental Internet content rating system. As discussed above, the governmental Internet content rating system has raised unnecessary censorship issues. In the long term, this can be an obstacle to developing even the voluntary Internet content rating system.

Q10. In your opinion, which of the following organisations ought to operate the Internet content rating system? Tick or complete all relevant options.

	%.	No.	
Academic Expert Group	16	16	
Government	11	11	
Internet Industry	22	22	
Civil Organisation	**36**	**36**	
Not-answered	15	15	
Total		100	

Table 8.8. The result of the questionnaire [Q10]

The majority of respondents, 36 percent, considered civil organisations to be the most suitable for operating the Internet content rating system. Although ICEC, a governmental institution, is currently operating its own Internet content rating system, the government comes lowest with 11 percent. This result indicates that the civil sector has succeeded in gaining respondents' trust in terms of Internet content regulation, while the government seems to have failed to do so.

8.5.4. Section III: The Harmful-to-youth Medium Material Indication System

The third section of the questionnaire consists of five questions that ask respondents about their knowledge and opinions of the harmful-to-youth medium material indication system. The results are as follows:

Q11. Have you heard about the harmful-to-youth medium material indication system? (*If YES, please answer to all questions from Q12 to Q15. If NO, please go to Q16*)

	%	No.	
Yes	**88**	**56**	
No	10	6	
Not-answered	2	1	
Total		63	

Table 8.9. The result of the questionnaire [Q11]

Compared with the conventional Internet content rating system, 13 percent more of the respondents claimed knowledge of the harmful-to-youth medium material indication system. In my view, the reason for this figure is that the harmful-to-youth medium material indication system is a mandatory system which imposes punitive sanctions (see Chapter 7.1.3), while other rating systems, including the ICRA system and the SafeNet system, are self-regulatory systems based on people's voluntary participation. The harmful-to-youth medium material indication system has raised several contentious issues as discussed in the previous case studies (see Chapters 8.2. & 8.3).

Q12. How confident are you about using the harmful-to-youth medium material indication system?

	%	No.	
Very confident	17	11	
Fairly confident	36	19	
Not at all confident	**42**	**26**	
Not-answered	11	7	
Total		63	

Table 8.10. The result of the questionnaire [Q12]

42 percent of respondents answered that they are *not at all confident* about using the harmful-to-youth medium material indication system. This number is

exactly the same as the number of respondents (but not the same people) who answered "*not at all confident*" to question Q6 which asks about the respondents' knowledge of the Internet content rating system. Although the percentage of respondents who are *not at all confident* is 2.5 times greater than the percentage who are *very confident*, the number of respondents with some degree of confidence is greater than the number of those who are diffident about using the system.

As with question Q6, in these responses "*not at all confident*" can be interpreted as meaning that respondents merely know the name of a system but lack any detailed knowledge. This figure is quite disappointing, since in the previous question almost 90 percent of respondents answered that they have heard about the system. Among 56 respondents who replied "*yes*" to question Q11, almost half of them, 26 respondents, answered that they are *not at all confident* in using the system. To summarise, in this sample the majority of respondents who are in charge of Websites lack proper knowledge of the harmful-to-youth medium material indication system, although the system imposes punitive sanctions.

Q13. Would you classify the harmful-to-youth medium material indication system as an Internet content rating system?

	%	No.	
Yes	**67**	**42**	
No	17	11	
Don't know	6	4	
Not-answered	10	6	
Total		63	

Table 8.11. The result of the questionnaire [Q13]

ICEC has claimed that the harmful-to-youth medium material indication system is not a rating system. However, opponents recognise it as a compulsory Internet content rating system, since it is based on the PICS standard and grammar on which most Internet content rating systems rely on. In my view, it is not a conventional Internet content rating system, but can be classified as a modified Internet content rating system as long as it is based on the PICS technical standard. The most important difference between them is that the system provides only one designated value, while the conventional rating system provides various levels of information on the Internet. The harmful-to-youth material medium indication system gives end-users only two descriptors: blocking the harmful-to-youth material or allowing it (see Chapter 7.2.2).

In their responses to this question, the majority of respondents answered that it is an Internet content rating system. 67 percent of the respondents said "*yes*," while 17 percent of the respondents said "*no*." This result confirms my opinion that the harmful-to-youth medium material indication system is a modified or applied Internet content rating system (see Chapter 7.2.2).

In question Q9 the majority of respondents opposed the idea of a governmental institution operating the Internet content rating system. Ironically, in this question the majority of respondents see the harmful-to-youth medium material indication system as a governmental rating system. Civil organisations, such as the JINBO Network Centre, have criticised the government for operating the mandatory rating system to regulate Internet contents in the name of protecting minors, while in fact it works as a censorship tool (see Chapter 7.5).

Q14. The harmful-to-youth medium material indication system is an efficient technical solution to protect minors from harmful information on the Internet. Do you agree?

	%.	No.	
Strongly agree	5	3	
Agree	27	17	
Disagree	**30**	**19**	
Strongly disagree	6	4	
Unsure / Don't know	22	14	
Not-answered	10	6	
Total		63	

Table 8.12. The result of the questionnaire [Q14]

Alongside 27 percent of respondents who *agree* or *strongly agree* with the above given statement, a significant number of respondents, 36 percent, answered that they *disagree or strongly disagree*. This figure indicates that it is highly controversial whether the system is an efficient technical solution to prevent minors from being exposed to harmful information on the Internet. It has been three years since this system was first introduced in 2001. However, it has not had any significant effect on issues of harmful information on the Internet, even though it imposes heavy penalties. In contrast, these issues are getting more serious and more widespread. In my view, this is the main reason for respondents' distrusting the efficiency of the system.

Q15. The harmful-to-youth medium material indication system may violate freedom of expression on the Internet. Do you agree?

	%.	No.	
Strongly agree	11	7	
Agree	22	14	
Disagree	**38**	**24**	
Strongly disagree	11	7	
Unsure / Don't know	8	5	
Not-answered	10	6	
Total		63	

Table 8.13. The result of the questionnaire [Q15]

Despite many contentious incidents related to this system, such as the EXZONE case (see Chapter 8.2), almost half of the respondents did not think that the system could violate freedom of expression on the Internet. In my view, the reason for this figure is that this system directly aims at protecting minors on the Internet, an initiative which has already gained widespread public acceptance. However, over one third of the respondents identified that the system has negative effect on freedom of expression on the Internet.

8.5.5. Section IV: Labelling and Rating

This is the final section of the questionnaire which asks the respondents about labelling and rating issues.

Q16. At present, do you label your site with any Internet content rating system including the harmful-to-youth medium material indication system? (*If YES, please answer all questions from Q18 to Q25. If NO, please answer to Q17*)

	%	No.	
Yes	10	6	
No	**82**	**52**	
Not-answered	8	5	
Total		63	

Table 8.14. The result of the questionnaire [Q16]

As mentioned in question Q4, the Internet content rating system cannot work properly at such a low rate of site-labelling. In this sense, these figures can be interpreted as an indication that no Internet content rating system is effectively working at the moment in South Korea. As of April 2005, ICEC is the only institution in South Korea to operate such a system.

Q17. If NO, why not?

	%	No.	
Unnecessary	**53**	**28**	
Technical difficulty	4	2	
Not informed	35	18	
Other	8	4	
Total		52	

Table 8.15. The result of the questionnaire [Q17]

The most common reason for not labelling was that the respondents thought that labelling their sites was *unnecessary*. Ironically, almost one-third of the respondents who answered "*unnecessary*" previously agreed or strongly agreed with the statement in Q7 that the rating system is an efficient technical solution to protect minors from harmful information on the Internet. The same number of respondents who supported the harmful-to-youth medium material indication system in question Q14 also replied that they do not feel a need to

label their sites using the rating system. These correlative figures show that many people who are theoretically in favour of an Internet content rating system do not, in practice, apply the system to their site.

Nine of the respondents who said "*unnecessary*" were interviewed via e-mail.[22] Through the interviews it emerged that most of them misunderstood the mechanism of the Internet content rating system. They wrongly believed that rating and labelling were only for some specified Websites which deal with explicit adult information. In this context, they did not feel a need to rate and label their sites. One of them said, "My site does not provide any explicit adult information nor harmful-to-youth information, but only legitimate information. My site never experiences any trouble with the authorities. Why should I rate and label my site?" (Respondent No. 5) Another respondent said, "My site is only for educational purposes for my students. I never feel a need to label it." (Respondent No.43)

In my view, the existence of this mandatory system gives people an inaccurate concept of the Internet content rating system. Not many people realise that the Internet content rating system is a technical self-regulatory solution for dealing with harmful Internet content. Also they do not know that it was initially designed to be based on information providers' voluntary rating and labelling. Instead, people wrongly conclude that it is one of the mandatory regulation systems which are only applicable to certain problematic Websites. In this context, most people who provide moderate contents do not feel any need to use the Internet content rating system at all. They do not recognised that the system cannot have practical force unless the number of rated sites reaches a critical mass.

---

[22] The interviews were conducted via e-mail from 10th March 2003 to 15th March 2003.

The second reason for not labelling Websites was "*not informed.*" Among the 18 respondents who replied "*not informed,*" 11 respondents answered in the earlier question Q4 that they had heard about the Internet content rating system. Similarly, 15 out of the 18 respondents previously replied that they know of the harmful-to-youth medium material indication system in question Q11. The former 11 respondents represent almost a quarter of those who answered that they know of the rating system. The latter 15 respondents equate to over quarter of the respondents who replied that they know the harmful-to-youth medium material indication system. Thus, these correlative figures can be interpreted as meaning that a significant number of people do not properly understand that information providers and users' voluntary participation is critical to the success of the Internet content rating system, although they have at least a superficial knowledge of the system.

Q18. If YES, why do you label your site with the Internet content rating system(s)?

	No.
By recommendation(s)	0
By my (company's) own decision	3
By legal order(s)	3
Other	0
Not-answered	57
Total	63

Table 8.16. The result of the questionnaire [Q18]

Since six respondents answered "*yes*" to question Q16, there could be only six responses to questions Q18 to Q25. The reasons given by respondents for labelling their sites are as follows: three respondents answered that they labelled their sites on their own initiative and another three respondents

labelled their sites by legal order. The legal order means ICEC's administrative order under *Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.*

As discussed in Chapter 7, if a certain Website is classified into a harmful-to-youth medium material by ICEC, the site's owner has an obligation to mark his/her site as a harmful-to-youth medium using text, graphic and electronic methods together. If the owner does not comply with this, he/she can be sentenced up to two years' imprisonment or punished with a fine up to 10 million KRW (about 5,400 GBP) (see Chapters 7.1.3.2 & 7.2.2). However, as established by studying the EXZONE case, this procedure has been quite problematic.

Q19. How many Internet content rating systems are you using at present?

	No.
1	3
2	1
More than 2	2
Not-answered	57
Total	63

Table 8.17. The result of the questionnaire [Q19]

The systems which the six respondents specified are as follows: SafeNet, ICRA, RSACi, SafeSurf and the harmful-to-youth medium material indication system. No respondents use the Safety Online system which is ranked as the second most well-known system in question Q5. Although the number of respondents is very small, this study at least supports my assumption that the Safety Online system has become the second most well-known system, largely because of confusion between two systems which have very similar names: the Safety

Online system and the SafeNet system.

Q20. Did you apply the label to the whole site or to specific pages?

	No.
Whole site	3
Specific pages	3
Not-answered	57
Total	63

Table 8.18. The result of the questionnaire [Q20]

The Platform for Internet Content Selection (PICS) which is a technical standard of the Internet content rating system allows users to apply a label to a whole site or to specific pages (see Chapter 5.2.1). It is unnecessary to label a whole site in the same way because Web pages even under the same domain can contain different content.

Of the respondents who use such systems, half (three in each case) answered that they applied the label to the whole site and to specific pages respectively.

Q21. Have you experienced any technical difficulty concerning rating and labelling on your site?

	No.
Yes	1
No	5
Not-answered	57
Total	63

Table 8.19. The result of the questionnaire [Q21]

Only one respondent answered that he/she experienced technical difficulties,

while the rest of the respondents never experienced any technical difficulties. In question Q 17, a mere two respondents replied that they did not label their sites because of technical difficulties. In this sense, it can be said that rating and labelling processes are straightforward and do not require a high standard of technical expertise. In practice, most current rating systems provide an automatic labelling system or labelling templates.

Q22. Does the Internet content rating system provide enough rating categories and descriptors for classifying your site?

	No.
Yes	2
No	4
Unsure / Don't know	0
Not-answered	57
Total	63

Table 8.20. The result of the questionnaire [Q22]

The SafeNet system provides five categories on scalar numbers of levels. In my view, however, this kind of rating template inevitably involves some degree of value-judgment. Moreover, it cannot fully reflect the complexity of human language. As an alternative, the latest ICRA system lists all vocabulary elements which are applicable to their Web content. It does not yet constitute a perfect solution, although it is an upgraded system compared to other previous rating systems (see Chapter 5.3.3). Since the Internet has been developed as a global architecture, the Internet content rating system's categories and descriptors need to be globally translatable. However, it may be impossible to develop a perfect global system, because a descriptor can be interpreted in various ways, according to different socio-cultural backgrounds all over the world.

Q23. How long in total did it take to label your site?

	No.
less than 1 hour	4
1-4 hours	2
4-8 hours	0
more than 8 hours	0
Not-answered	57
Total	63

Table 8.21. *The result of the questionnaire [Q23]*

This result shows that rating and labelling are not a time-consuming job.

Q24. After labelling your site, has there been any change to your Website's traffic?

	No.
None	4
Increase	0
Decrease	2
Unsure / Don't know	0
Not-answered	57
Total	63

Table 8.22. The result of the questionnaire [Q24]

Two respondents who said that after labelling their Website the traffic had decreased are both working for Websites which are classified into the *entertainment* category. Also, they both labelled their sites in response to a legal order. Through e-mail interviews with these two respondents[23] it was

[23] These e-mail interviews were conducted on 17th and 18th March 2003.

found that the changes in traffic were not significant and did not have any practical effect on their sites. Unfortunately, they were not able to provide detailed data about the changes. It has not been possible to confirm how much the labelling of a site affects its traffic because the number of respondents to whom this question applied was too small. However, from the study at least, it appears that labelling a site hardly has any practical effect on the traffic of the sample sites. It confirms my previous argument in the EXZONE case study that the mandatory labelling system has less impact on adult content sites, since most legitimate commercial adult content sites have provided adult verification devices for commercial purposes, even before the system was introduced. Furthermore, such sites are accessed in privacy rather than at public places where PICS-compatible filtering software is obligatorily installed (see Chapter 8.2).

Q25. Have you ever revised your site's contents in order to get a certain degree of rating?

	No.
Yes	2
No	4
Not-answered	57
Total	63

Table 8.23. The result of the questionnaire [Q25]

Of two respondents who replied "*yes*," one respondent's site is an online-game site which has different age groups making up its audience from early teens to adults. This site was labelled by legal order. Presumably, if it had not changed its contents it might have been labelled as harmful-to-youth site. The site would then have been in danger of losing its major audience – teenagers.

In my view, if someone changes his/her site's contents in order to get a certain degree of rating, it can be said that he/she conducts self-censorship on his/her own contents. This is an unintended side-effect of the Internet content rating system. On the one hand, it can be said that the system encourages people's self-regulatory efforts, while on the other hand the criticism can be made that it works as an invisible force to restrict freedom of expression on the Internet. Even if someone has not changed his/her site's contents to get a certain preferred degree of rating, there is still another problem. As mentioned in the previous chapter (see Chapter 5.6), there is always the potential for people to cheat in their self-rating. Furthermore, mis-rating can happen unintentionally, because many Web pages contain very complex information. Most Internet content rating systems largely rely on the concept of self-rating so they are running without a penalty system. In this sense, the Internet content rating system may break down without the existence of punitive sanctions. For the same reason, the ACLU (1997) makes the criticism that the rating system will encourage some degree of governmental intervention on the Internet.

8.5.6. Findings

The four major findings of the questionnaire are as follows:

The first finding is that the Internet content rating system in South Korea is still insufficiently well-known. The system has been underused and even people who have Internet-related job titles lack proper knowledge of the Internet content rating system. Consequently, the system has not made a big impact because of the low rate of site-labelling.

Secondly, the public's attitude to the idea of an Internet content rating system is ambivalent. In the questions about the rating system's effectiveness and

freedom of expression, the respondents' answers were evenly split. While half of them took a negative attitude to the system, the other half recognised it as an efficient tool for preventing harmful Internet content. Therefore, it is still highly debatable whether the Internet content rating system is an efficient technical solution to protect minors from harmful information on the Internet.

Thirdly, a majority of the respondents oppose the government-centred Internet content rating system and choose non-governmental organisations as the most suitable bodies for operating the rating system. Even many respondents who supported the rating system did not select the government as an appropriate rating body, although the governmental agency, ICEC, is the only institution which operates the rating system in South Korea as of April 2005.

Fourthly, the mandatory system is an obstacle to people's voluntary participation in the Internet content rating system because it gives people an inaccurate concept of the system, which it is one of enforced regulatory tools used to deal with problematic Websites.

As mentioned above, this survey is based on 63 usable responses which represent 9.56 percent of the 659 samples. The number of respondents in the survey is small compared with the number of the target population, so it is regrettable that the results of this questionnaire cannot firmly represent the South Korean Internet population's opinion about the Internet content rating system.

8.6. Conclusion

The South Korean government has made great efforts to develop its Internet infrastructure. As a result, South Korea has become the world's leading country

in terms of Internet usage and infrastructure, in particular broadband Internet access (see Chapter 6). The South Korean public is very proud of this significant Internet development. They call their nation "the Internet superpower nation." No one denies that the government's strong support for the Internet industry has played an important role, although this remarkable achievement cannot be explained solely in terms of the government's pro-Internet policies; social factors have also played a very significant part. However, the South Korean government's restrictive attitude towards Internet content regulation casts a shadow on this success story.

As mentioned in the two case studies, the mandatory Internet content rating system has raised many controversial issues and has been strongly criticised by a number of civil organisations. Although it was introduced to deal with harmful-to-youth information on the Internet, in practice it works as a governmental censorship measure. In particular, the voices of social and sexual minorities on the Internet have been virtually censored by the government. The result of the questionnaire shows that a majority of respondents oppose this mandatory rating system which forces certain information providers to rate their information. In spite of its many vocal critics, the government has refused to budge on its strict Internet content regulation policies. ICEC' budget is still increasing year by year and it still restricts all kinds of information on the Internet, from political information to copyright issues.

As discussed in the previous chapters, illegal content is primarily a matter of law enforcement. In my view, the major problem of Internet content regulation in South Korea is that the government actively interrupts the circulation of Internet content which is legal but deemed to be harmful. Although the South Korean Court has made a distinction between illegal and harmful content (see Chapter 2.4), the governmental Internet content regulatory body regulates

sensitive social or political expression which is protected under the Constitution with the ambiguous regulatory concept, the so-called "improper communication" of Article 53 of *the Telecommunications Business Act*. This trend of the South Korean government's presents a striking contrast to Internet content regulation in many Western countries which favour a form of co-operative regulation which is conducted jointly by end-users, Internet industry and government. As discussed in the previous chapter, the UK and the European Union has endorsed industry-based self-regulation rather than governmental regulation in terms of regulating harmful Internet content, while they have also applied governmental regulation to issues of illegal Internet content.

In the next chapter I shall discuss detailed policy implementations regarding Internet content regulation in South Korea.

CHAPTER 9

A STEP TOWARDS THE NEW INTERNET CONTENT REGULATION IN SOUTH KOREA

9.1. Introduction

As mentioned in the previous chapter, for the past few years, many governments all over the world from the US to China have attempted to regulate and control content on the Internet in various ways. However, most of these attempts have turned out to be inefficient in preventing minors from exposure to harmful information on the Internet. In some cases it raised serious censorship issues. The South Korean government has been one of these governments. Furthermore, it is a prime example, since it adopted a government-centred Internet content regulatory system and also introduced the first governmental Internet content rating system in the world. In this chapter I shall analyse the reasons for the absence of an Internet self-regulation system in South Korea, and discuss issues relating to the implementation of its new Internet content regulation policy.

9.2. Article 53 of the Telecommunications Business Act and the Korean Constitutional Court[1]

In June 2002 the Korean Constitutional Court made a significant decision which for the first time restrains the government-centred Internet content policy (Judgment of June 27, 2002, 99Hun-Ma480, 14-1 KCC 616). The Court ruled Article 53 of *the Telecommunication Business Act* which has provided the major authority for the government-centred Internet content regulation as unconstitutional. As discussed in Chapter 7, Article 53 had raised controversy during the previous years. It defines the Ministry of Information and Communication (MIC) Minister's refusal, suspension and restriction order against "improper communications" and provides a legal basis of the

[1] The full text of the Korean Constitutional Court's decision is available in English at http://www.ccourt.go.kr/english/download/decision_2003.pdf (Retrieved April 6, 2005)

Information Communication Ethics Committee (ICEC). Under this provision, ICEC shut down a number of Websites, including Kim In-Kyu's homepage, iNOSCHOOL, non-serviam.org and IVANCITY.

In this case, the Court judged whether Article 53 violate the rule of clarity, the rule against excessive restriction and the rule against blanket delegation. In addition, the Court examined the constitutionality of the MIC Minister's refusal, suspension and restriction order against "improper communications."

Firstly, Article 53(1) of *the Telecommunications Business Act* defined "improper communications" as "communication with contents that harm the public peace and order or social morals and good customs." The Constitutional Court held that this provision violates the rule of clarity which is "especially important in legislation that regulates freedom of expression," because the concept of improper communication is unclear, ambiguous and abstract:

> Since "the public peace and order" and "the social morals and good customs" are such abstract concepts, different individuals may make different judgments about whether a particular expression is harmful to "the public peace and order" or "the social morals and good customs" because of differences in individuals' value systems or moral values. Furthermore, it would be difficult to objectively define their meaning through an ordinary interpretation of law by enforcement agencies (Constitutional Court of Korea, 2003, p. 65).

Secondly, the Court made a clear distinction between harmful and illegal content and ruled that the concept of improper communication violated the rule against excessive restriction:

> Article 53 of the Act could be used to regulate "indecent" expression which this Court has explicitly held to be protected under the

> Constitution (10-1 KCCR 327, 95Hun-Ka16, April 30, 1998),[2] citing that these expressions are against "social morals and good customs." (p. 66)
>
> It could be employed to regulate expressions regarding sexuality, marriage, or the family system (i.e. expressions regarding living together before marriage, contractual marriage, or homosexuality) for harming "social morals and good customs," and it could be used to regulate expressions regarding sensitive political or social issues (i.e. expressions about opposition to conscription, conscientious objection to war, reunification issues), by labelling them as harmful to "the public peace and order." This would inevitably have a chilling effect on the users of telecommunication services, and open discussions would be impossible for some social issues. This would violate the essential features of the freedom of expression. (p. 67)

Thirdly, Article 53(2) of *the Telecommunications Business Act* prescribed, "The objects, etc. of the communication, which are deemed harmful to the public peace and order or social morals and good customs under paragraph (1), shall be determined by the Presidential Decree." The Court judged that this provision violated the rule against blanket delegation for the following reasons:

> [C]oncepts of "public peace and order" or "social morals and good customs" are very abstract and unclear, and the provision employing such terms does not provide citizens with even vague ideas about the criteria or basic contents of regulation by presidential decrees. [...] The instant statutory provision also does not provide appropriate guidelines to the administrative agency, and thereby fails to control administrative regulation properly. [...] Thus, the administrative agency could even regulate those expressions that should be protected under the Constitution according to its own judgment or preference about what the concepts of "the public peace and order" or "the social morals and good customs" should represent (p. 69).

Fourthly, the Court subsequently held Article 53(3) which articulates the MIC Minister's refusal, suspension, and restriction order to be unconstitutional, on

---

[2] see Chapter 2.5: Footnote 34. The case on *Registration Revocation of Obscenity Publishers.*

the basis of the above arguments.

Through this judgment, the Court criticised the vagueness and excessiveness of Internet content regulation, and underlined the importance of freedom of expression. The Court stated:

> "[T]he state should not give up its pursuit to uphold the rule of clarity through individualization or categorization. If this is not possible, the state must choose underregulating rather than excessively restricting expression." (p. 66)
>
> [R]egulation of expression on the Internet with emphasis on maintenance of order would be detrimental to the promotion of freedom of expression. Technological advance about the media continues to widen the scope of freedom of expression and brings about changes in the quality of such expression (p. 68).

A former Judge of the Seoul District Court, Lee Hae-Wan (2002) claims that this was a landmark decision for the South Korean Constitutional Court as it clarified for the first time its liberal standpoint of freedom of expression on the Internet. Professor Hwang (2003, pp. 118-119) also comments that this Constitutional Court's decision is significant in that it is the first legal examination of Internet content regulatory legislation in South Korea. Kim Ki-Joong (2003), a legal counsel of the JINBO Network Centre, claims that the Court made a historical judgment of unconstitutionality which is analogous to the judgment of unconstitutionality against CDA[3] in the US.

All three commentators discuss that the decision largely adopted the legal principle of the CDA case in 1996. Citing the judgment of the CDA case, the Constitutional Court stated that the Internet is "the most participatory media,"

---

[3] see Chapter 2.6.1.1. *ACLU v. Reno* 512U.S. No.96-511

or "media encouraging expression of individuals" (p. 68). As the US Supreme Court held that the Internet is not an invasive broadcast medium, the Constitutional Court also claimed that the Internet does not have the equivalent characteristics of broadcasting media, such as scarcity of radio wave frequencies and pervasiveness of broadcasts.

Although it took three years to reach this conclusion after the case was filed in August 1999, this decision was welcomed and supported by many civil organisations and experts.[4] Indeed, they expected that as a result of the Court's decision, the government might change its Internet content regulation policy to something more akin to self-regulation.

9.3. Reformed Bill of Article 53 of the Telecommunications Business Act

The unconstitutional decision on Article 53 inevitably led to a new regulatory approach, since the provision provided the major legal ground for regulating obscene materials on the Internet. ICEC lost the legal foundation of its deliberation system which relied on the concept of "improper communication" and its functions were hamstrung. However, not everyone welcomed this situation. Some people voiced their concern about absence of Internet content regulatory regime ("JEONGBO TONGSIN YUNRIWI", 2002). The government hurried to reform the provision; only one month after the unconstitutional decision a reformed bill was introduced without any open public debate.

However, the reformed bill immediately faced strong challenges (INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE,

[4] The JINBO Network Centre (2002a) and the Internet Self-Regulation Forum (2002a) both announced their statements which welcome the Court's decision.

2002b). Although it abandoned the concept of "improper communication" and clearly defined the objects of regulation in the name of "illegal information" instead, it retained the MIC Minister's right to refusal, suspension and restriction order against "illegal information" which can be made without first obtaining a court order.[5]

Kim Ki-Joong (2003) argues that "illegal information" under the amended *Telecommunications Business Act*[6] still includes vague contents so that the Act can be applied without much difference from the regulation on "improper communication." He also argues, "there is no difference basically from the system prior to the amendment to the law in the aspect that MIC and ICEC

---

[5] Amended Article 53(2) of the amended *Telecommunications Business Act* reads as follows:

> [...] the Minister of Information and Communication may order the relevant telecommunications business operator to reject, discontinue or limit the use of such telecommunications after going through deliberation thereon of the Information Communication Ethics Committee that is formed in accordance with Article 53-2.

[6] Article 53(1) of the amended *Telecommunications Business Act* reads as follows:

> (1) Any person who uses the telecommunications shall be prohibited from performing an act falling under each of the following subparagraph: **1**. The act of distributing, selling, renting or publicly exhibiting the telecommunications whose contents carry obscene codes, letters and languages, sounds, images or films; **2**. The act of using the telecommunications whose contents defame other person's honor by publicly revealing actual facts or false facts about him for the purpose of slandering him; **3**.The act of using the telecommunications whose contents carry codes, letters and languages, sounds, images or films that incur fears and uneasiness, and are repeatedly sent to the other party; **4**.The act of using the telecommunications whose contents damage and destruct or forge information and communications system, data or programs and obstruct their operation without any justifiable grounds; **5**.The act of using the telecommunications whose contents carry the media information prescribed as harmful to juveniles by the Juvenile Protection Act and are offered for the purpose of profit without fulfilling the obligations provided for in the Acts and subordinate statutes, including the obligation of confirming the age of the other party and the obligation of indications, etc.; **6**.The act of using the telecommunications whose contents fall under the speculative act that is banned under the Acts and subordinate statutes; **7**.The act of using the telecommunications whose contents leak the State's secrets, including other secrets classified under the Acts and subordinate statutes; **8**.The act of using the telecommunications whose contents perform the act that is banned under the National Security Act; and **9**.The act of using the telecommunications who contents are aimed at instigating or abetting crimes.

keep holding the power to conduct the examination."

The JINBO Network Centre (2002b) argues that the reformed bill misunderstands the Constitutional Court's decision. In particular, it claims that retaining the MIC Minister's veto power still violates the constitution, because such an administrative order in effect exercises a judicial power, although only "illegal information" could be its subject. An expert report which was commissioned by the Science, Technology, Information and Telecommunication Committee (STITC) of the National Assembly (2002) also indicated the same problems. The report states:

> Although the reformed bill is made up for the weak points, including a condition of the regulatory object and legality of the regulatory procedure, the essence of the regulatory system still remains. As the Constitutional Court points out, content regulation which is directly related to freedom of expression is conducted under the MIC minister's administrative authority, not by the judicial authority.

As the Constitutional Court (2003, p. 66) states, "necessity of such regulatory measures as deletion of messages cannot be denied considering the rapid speed of online information dissemination." However, Professor Hwang (2003, p. 133) argues that there are certain dangers in an administrative institution arbitrarily judging the illegality of Internet content, in particular content which is related to issues of obscenity and national security. The regulatory object of European hotlines is much narrower as compared with ICEC (the notice and take down procedure of hotlines in Europe was critically appraised in Chapter 3). However, they have been criticised for lack of transparency and accountability, since most hotlines are largely industry-based. As discussed, ICEC have also been subject to similar criticisms, although it is a governmental agency.

Although civil rights organisations strongly demanded the removal of the provision of Article 53 of *the Telecommunications Business Act*, the National Assembly adopted the bill as submitted by MIC (INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE, 2002b). The National Assembly passed this controversial reformed bill in November 2002. Kim Ki-Joong (2003) criticised the government and the National Assembly for abandoning the best chance to establish a reasonable model for Internet content regulation.

In my view, the Constitutional Court's decision indicated a new trend in Internet content policy in South Korea. However, building a new regulation system is not an easy job and it cannot be completed in a short time. It requires the co-operation and long-term efforts of all the major parties that are involved in the regulation system.

9.4. Co-Regulation of Internet Content and South Korea

In the previous chapters, I discussed the co-regulation model that has been adopted by the EU and a number of self-regulatory institutions in Europe (see Chapter 2.6.4.2, 3.4 & 3.5). Although this co-regulation model is still not satisfactory,[7] in my view this regulation model has a number of advanced features. First of all, it is based on the participation of all the major parties from government and Internet industry through to end-users. Secondly, it makes a distinction between illegal content and harmful content and takes different regulatory approaches to each issue, so that governments do not excessively

[7] For instance, as discussed in Chapter 4 and 5, technical solutions, such as Internet content filtering software and the rating system, which are part of co-operative regulation model have been criticised for a number of reasons from technical weaknesses to freedom of expression issues.

regulate content which may be harmful to certain people, but protected by law. In particular, this model emphasizes the empowerment of users, while it circumscribes government's role in supporting self-regulatory efforts and dealing only with illegal matters. Nevertheless, many difficulties need to be overcome before a co-regulation model can be applied to a new Internet content regulation system in South Korea, since its social and political environment is quite different from the situation that exists in Western countries.

As discussed in Chapter 6.3, in South Korea a number of governmental institutions have exercised content regulation of each distinctive medium area from publication to sound records and films. During the period of Bak and Jeon's military regimes all the media were subject to these governmental agencies' prior censorship. As of 2005, the government does not restrain freedom of expression on the media through a prior examination any more, although prior deliberation is still applied to films, video and game products. Since the Kim Yeong-Sam administration formally opened the civilian form of government in 1992, regulation on traditional media has tended to be loosened, although change is quite slow (K. Kim, 2003).

However, even today most governmental regulatory agencies are exercising a certain degree of restraint on the media through post-deliberation (Hwang & Hwang, 2003; K. Kim, 2003). In terms of content regulation the Korean Internet industry has no accumulated experience of self-regulation, since the tight governmental content regulatory system has not left room for the Internet industry to establish its own self-regulatory scheme (Hwang, Hwang, Kim & Choi, 2004, pp. 184-185).

In sum, in South Korea the social and political infrastructures for supporting

the co-operative Internet content regulation model are not yet in place. However, despite the present lack of these infrastructures, the co-operative model is in my view the most desirable model. I believe that in the foreseeable future the South Korean government is very likely to follow this new trend. The Constitutional Court's decision on Article 53 of *the Telecommunication Business Act* would accelerate the regulatory tendency which aims to be less restrictive than the previous system. Now is the time for designing a new Korean Internet content regulation policy based on the co-regulation system which has been developed in many Western countries. In the next section I shall discuss a policy proposal for Internet content regulation in South Korea.

9.5. The Absence of a Self-Regulation System in South Korea

Before we discuss a new policy, it is necessary to examine the reasons for the absence of a self-regulation system in South Korea. The Internet Self-Regulation Forum, the so-called R3Net group, points out five major reasons for it in its report, *For the new start of the Internet content regulation policy* (Internet Self-regulation Forum, 2002b) as follows:[8]

Firstly, since the South Korean government has played a dominant role in the Internet content regulation system, the South Korean civil sector does not have any accumulated experience of self-regulation. For instance, no civil organisation operates a watchdog system against illegal information on the Internet. Their critical activities on the media are not powerful enough to exercise influence over the public. The Internet industry's self-regulatory efforts have not taken effect as yet.

---

[8] I myself am a board member of the Internet Self-Regulation Forum. I joined the Forum in March 2002 and now work voluntarily for the Forum as an international officer. For this reason, I took part in producing this report as a co-researcher.

Secondly, there are the legal and administrative obstacles to self-regulation. The existence of the government-centred content regulation, such as Article 53 of *the Telecommunication Business Act*, and the governmental deliberation institution which operates its own content rating system are prime examples. Thus, information providers have remained simply as an object of governmental regulation. They have not played an active role in the Internet content regulation system.

Thirdly, information consumers used to be in a passive position. The traditional media are defined by a strict division between providers and recipients. In the traditional media only providers transmit information to recipients and the content is always decided by the providers. However, with the advent of the Internet medium which is incredibly interactive, the difference between information providers and recipients has been blurred. In principle, all Internet users can be suppliers of content and not merely recipients. Millions of ordinary South Koreans, from teenage students to housewives, are running their own Websites and Web communities but they are still in a very passive position in terms of Internet content regulation.

Fourthly, there is no public consent about the aim of Internet content regulation. The issue about who holds the power of regulation has been a major concern. If the goal of Internet content regulation becomes clear and if the active participation of the major players is secured, then the question of who holds the power becomes just a matter of minor tactics. The government has claimed that its regulation is primarily aimed at preventing minors from being exposed to harmful material on the Internet. But its claim has not gained public consent, since governmental institutions have directly intervened not only in illegal content, but also in a wide range of other contents and activities on the Internet from political issues to copyright disputes. ICEC has been criticised for cyber

censoring. As mentioned in Chapter 7, from 1997 to 2002, the cumulative number of ICEC's deliberations on political matters was 3,607 (see Chapter 7.3). It shows that ICEC repeatedly intervenes in political activities on the Internet. In this sense it can be said that the government itself blurs its regulatory aim.

Fifthly, the various parties concerned cannot participate in the process of designing the Internet content regulation policy, since the South Korean government used to monopolise the decision process and the making of its policies. Although the parties who are directly affected by a certain governmental policy could be provided with institutional means of voicing their opinions, the South Korean government has failed to provide these opportunities. The government's unwillingness to include other parties in the policy-making process is evident in many instances; in particular it was highlighted in the debate over the controversial Article 53 of *the Telecommunication Business Act*. Unfortunately, in that debate the government ignored civil organisations and Internet experts. The government is still not close to providing a legal framework to ensure the participation of other concerned parties in Internet content regulation. Instead it is keeping the regulatory power to itself.

9.6. Towards the New Internet Content Regulation

9.6.1. A Role of the Government

Taking into account the above five major reasons for the absence of a self-regulation system in South Korea, we can see that the success and failure of Internet content self-regulation largely depends on the government. In other words the government's role is decisive, even in the self-regulation system

(Hwang, Hwang, Kim & Choi, 2004, pp. 4-8). The Internet Self-Regulation Forum (2002b) defines self-regulation as follows:

> It is not a noninterference nor deregulation, but it is a regulation in which the civil sector actively takes part in the traditional area of governmental regulation, and the government supports and supervises the civil sector's self-regulatory efforts. Therefore, it aims at developing rationality and efficiency of regulation.

Apart from the theoretical classification, in practice there is no dichotomy between self-regulation and governmental regulation. In reality, the ideal of a completely voluntary model of self-regulation is rare. Most self-regulatory bodies are subject to a certain degree of governmental scrutiny (Price & Verhulst, 2000, p. 135). The Internet industry is also subject to a degree of governmental regulation.

Therefore, the most important issue regarding the new Internet content regulation system in South Korea concerns the relationship between the government and the self-regulatory bodies. As Price and Verhulst (2000, pp. 140-141) argued, the precise nature of this relationship may differ between nations, depending on each nation's particular social and political environment. On the one hand, a self-regulation system can mainly be built under a government's plan and with its support. On the other hand, it can be a result of harmonious collaboration between the government and the civil sector (Baldwin & Cave, 1999, pp. 125-126). The government is not necessarily the dominant partner in Internet content regulation, although, equally, there is no reason why the government should be eliminated from the regulation system.

Despite this flexible relationship, one thing we have to ensure is that self-regulation does not replace governmental regulation. In other words, even if

the self-regulation system succeeds in taking root, the government assumes the decisive responsibility for keeping legal order on the Internet (European Commission Working Party, 1996). Just like in the real world, on the Internet there is illegal content and activities that only governments can effectively deal with. As discussed in the EU Action Plan, a self-regulatory scheme, such as a hotline, may aid governmental regulation against illegal Internet content, but it cannot fully encompass these governmental areas. Therefore, self-regulation cannot be a substitute for governmental regulation (Breyer, 1982, p. 157). As discussed in Chapter 3, self-regulation is not favoured under all circumstances. It has a number of weaknesses, such as a lack of public accountability, ineffectiveness of enforcement and restriction of competition. In this context, Akdeniz (2005) argues that a self and co-regulatory framework should be backed not only by government but also by industry and civil society representatives.

The Internet Self-Regulation Forum (2003) claims that in the Internet era the South Korean government is required to make the best use of the advantages of self-regulation in order to achieve its regulatory policy goals. First of all, in practice, the government needs to provide a legal ground for developing co-regulation of Internet content. The main roles of the government should be empowering the civil sector's self-regulation ability and building appropriate legal and administrative infrastructures. With this as its foundation, it would be able to produce a detailed and effective policy which commands public respect and consent. This would then support and supervise the civil sector's self-regulatory efforts. These governmental activities are essential in order to develop a co-operative regulation model in South Korea.

9.6.2. Responsibilities of the Internet Industry

Under the strict governmental Internet content regulation system, the Internet industry that is represented by Internet service providers, Internet content hosts and Internet content providers has been in a very passive position. It has not been able to develop its own self-regulation system, since its self-regulatory attempts have been ignored or rejected by the government. It has been one-sidedly subjected to governmental regulation.

However, now, the Internet industry needs to recognise that its passive attitude is not helpful to its future. Its strong self-regulatory efforts towards a safer Internet environment will result in positive rewards regarding the development of the Internet industry's business infrastructure. Previously every time an issue concerning appropriate Internet content or activities is raised, the Internet industry was blamed for it. Moreover, it was often threatened with lawsuits or prosecution. In my view, the main reason for this undesirable situation is because the South Korean Internet industry does not have any experience of self-regulation. Therefore, developing codes of conduct is an urgent task of the South Korean Internet industry in order to ensure that it acts in accordance with its social responsibility. However, such self-regulatory efforts may not be successful without the government's support, because only the government is able to not only secure self-regulatory bodies' enforcement power, but also prevent them from misusing self-regulatory power. As the National Consumer Council, UK (2000, p. 48) claimed, "self-regulation works best within a legal framework. [F]or self-regulation to work effectively, there may be a need for a concept of co-regulation which is underpinned by legal regulation."

In September 2002, the Korea Game Industry Alliance (KGIA)[9] introduced its code of conduct for the first time. As mentioned in the previous chapter, the South Korean Internet game market and industry have been growing rapidly. Now, online games are the nation's favourite entertainment. However, alongside online games' explosive popularity, the South Korean Internet game industry has been severely criticised, because it has been argued that online games are a bad influence on minors. In particular, they have been blamed for many negative effects from game addiction to crimes that are related to online game items (see Chapter 6.2.1.4). This has become an issue of serious social concern. At the beginning of 2002, the government initiated heated discussions about a preliminary deliberation system on online games. Despite the online game industry's opposition, the government officially introduced it on 1st July 2002. The famous online game 'Lineage' became the first target.

In October 2002 the Korea Media Rating Board (KMRB), [10] a content regulatory agency of the Ministry of Culture and Tourism (MCT), decided to designate 'Lineage' as suitable only for those aged 18 and over because of violence and adult content (Na, 2002a). The online games industry, including NCsoft, was shocked by this decision, largely because about half of the users are under 18, and will not be allowed to play the most popular online game when the rating comes into effect. In November 2002 KMRB re-classified 'Lineage' as only suitable for those aged 15 and over (Na, 2002b). This incident raised heated debates about whether KMRB's decision on 'Lineage' was appropriate. It created the momentum for establishing a self-regulatory

---

[9] The Korea Game Industry Alliance was established on 26th September 2002 by six industrial associations which represent about 150 game-related companies in South Korea as follows; Korea Game Venture Association, Online Game Industry Association, Korea Mobile Game Association, Korea Internet Game Association, Korea Mind Sport Olympiad, and Busan Game Association (Resource: KGIA Website. Retrieved June 15, 2004, from http://www.kgia.org).

[10] see Chapter 6.3.

body of the Korean Internet game industry, the Korea Game Industry Alliance.

However, while most Internet self-regulatory initiatives in European countries, such as IWF, were set up with the support of each government, KGIA has found it difficult to establish a fruitful relationship with the government. This situation is partly because the government has not provided a legal framework to ensure the participation of other non-governmental bodies in the regulation system, but it has conducted extensive prior and post-deliberations on the media. This is also partly because of overlapping regulation by government agencies, such as MCT, MIC and the Ministry of Commerce, Industry and Energy (MOCIE). MCT is in charge of PC games, while MIC and MOCIE oversee online games and arcade games respectively, but because of the diversity and complexity of games the ministries often find it difficult to establish consistent policies. For instance, the rating given by KMRB of MCT differed from the rating given by ICEC of MIC. Thus, although ICEC gave Lineage a general level rating in 2000, it was given a different rating by KMRB. However, it can be said that the online games industry is a pioneer of self-regulation in South Korea. Under these complicated circumstances its self-regulatory efforts, including its code of conduct, are significant. I expect that it will be the main model for other industry-based self-regulatory bodies in South Korea.

Under the aegis of appropriate codes of conduct, the Internet industry could make great efforts to protect minors from exposure to harmful information and to prevent the distribution of illegal content. In particular, if an Internet content host recognises that it is hosting illegal content, it would be obliged to immediately delete the content and report it to the relevant authority. Also, if a user makes a complaint to an Internet content host about content that it is hosting, it can take action regarding that content and inform the user of the

result. This kind of complaint-settling process is an example of a so-called "Internet hotline." The UK-based Internet self-regulation body, the Internet Watch Foundation, is a well-known hotline provider. (see Chapter 3.6.1.2) The hotline system is one of the most important elements in the co-operative regulation model — but the procedure of the industry-based hotline system needs to be carefully monitored by various third parties, from the government to Internet user groups, in order to prevent that "it turns hotline operators into self-appointed judges of law." (ACLU, 1999c)

Since the industry's codes of conduct are the only self-regulatory norms, even though the industry operates its own self-regulation, it does not mean that the industry is immune from all legal responsibilities. In other words, even if codes of conduct are working successfully, the industry is never exempt from its legal obligations concerning Internet content. This is one of the self-regulatory system's limitations. For this reason, self-regulation most definitely needs legal and political support from the government.

In practice, the Internet industry's self-regulatory activities need to be carefully monitored by the government, civil organisations and the Internet industry itself. As mentioned in Chapter 3, there have been criticisms on self-regulation for its lack of accountability and democracy. There is always the possibility that the self-regulatory body may misuse its power for its own purposes, rather than the public interests it is supposed to safeguard. Therefore, the industry's self-regulation needs to gain public respect and consent, otherwise it may raise a private censorship issue.

As of February 2004, most major Korean Internet service providers, such as Korea Telecom, Hanaro Telecom and ThruNet, filter adult Websites which service in Korean, but are hosted abroad at the server level, without most end-

users being aware of this ("EUMRANMUL JEOPGEUNEUN", 2004). Even if they block only controversial adult sites in the name of protecting minors, these filtering actions cannot be justified, because they do not gain the consent of their adult end-users who have a right to access adult information as long as the information is lawful.

9.6.3. Empowering End-Users

Traditionally, the word "literacy" refers to the ability to read and write. However, in the Internet era, its implication has been ever more extended. It does not only refer to its traditional meaning. Nor does it imply the simple possession of the technical knowledge or skills for surfing the Internet. Since the Internet has provided end-users with the highly interactive communication environment (see Chapter 1.3), their participation is one of the most essential elements for maintaining the Internet. Thus, end-users' attitude and ability to understand and to control the Internet is decisive in making the Internet a better medium. Laura J. Gurak (2001, p. 16) defines literacy on the Internet, so-called cyber-literacy, as follows:

> To be cyberliterate means that we need to understand the relationship between our communication technologies and ourselves, our communities, and our cultures.

In my view, apart from its traditional meaning, Internet literacy implies the ability to understand the social, cultural and technical aspects of this important new communications medium, and also the ability to participate in it as critically-aware information consumers and providers. In this context, strengthening end-users' cyber-literacy is an essential element in the co-operative model. However, this task cannot be achieved in the short term: rather it is a long-term task. In my view, the best solution is to deal with

problematic Internet content in the long-term as compared to present day technical solutions that are less than ideal. Therefore, each party involved in the regulatory system is encouraged to make its best effort to reinforce it through continuous education and awareness campaigns.

9.7. Conclusion: The Korean "R3 Net" Strategy

In September 1996 the UK government, the Metropolitan Police, the Internet Service Provider Association UK, London Internet Exchange and the Safety-Net Foundation jointly agreed to a proposal called the *R3-Safety Net* to address the question of illegal material on the Internet, with particular reference to child pornography. The proposal's approach incorporates three key elements: rating, reporting and responsibility. Based on these principles, the proposal's regulatory mechanism can be described as follows: while the government retains "responsibility for law enforcement," the industry implements "reasonable, practicable and proportionate measures to hinder the use of the Internet for illegal purposes" and also provides "a response mechanism in cases where illegal and implement material or activity is identified." On the other hand, "end-users hold responsibility for the content they place on the Internet, whether legal or illegal." (ISPA UK, LINX & the Safety-Net Foundation, 1996) This kind of co-operative Internet content regulation system is adopted by the EU 'Action Plan for Promoting Safer Use of the Internet.' (see Chapters 2.6.4.2 and 3.5)

Taking into account the given Internet environment, which is ever more interactive and global, Akdeniz (2001c, p. 304) argues, "a multi-layered approach with the involvement of both public and private regulatory bodies at both national and international level is inevitable to deal effectively" with illegal and harmful content on the Internet. Professor Shim proposes (2002, pp.

72-73) that ISPs, users and the government should co-operate in making "criteria in terms of laws, technologies and norms," and underlines that the government should initiate such a co-regulatory scheme. In this context, co-regulation of Internet content would be a rational alternative to the current government-centred regulation system in South Korea. In order to establish the co-regulation system in South Korea, all the concerned parties, from the government to end-user groups, would be required to actively participate in Internet content regulation system. In conclusion, the following three essential strategies are required.

Firstly, the government would *reform* its Internet content regulation policy in a decisive manner. It is recommended that a legal framework is provided which supports and strengthens other parties' self-regulatory efforts. It is desirable that many different social groups, from the Internet industry to civil organisations, are stakeholders and participate in the Internet content regulation system, because this will encourage more people's active participation in the system. Furthermore, the government's deliberation system and its Internet content rating system would be abolished in order to prevent unnecessary censorship issues. In the long term I think these changes will result in ensuring public trust and in gaining public consent about its Internet content policy. Also, the ICEC, a controversial governmental deliberation institution, would renounce its deliberation function and change itself into an Internet hotline body – since 1997 it has operated its own Internet hotline, "Cyber Harmful Information Report Centre," which was renamed "Internet 119" in 2003. It also joined INHOPE as an associate in May 2003. Over the longer term it is anticipated that it would be a collaborative institution, neither appointed nor controlled by the government. Kim Ki-Joong argued (2003) that a change in Internet content regulatory policy may be quite slow, but it clearly tends to be less restrictive. In my view, the Constitutional Court's decision on Article 53 of

the Telecommunications Business Act is a landmark of this regulatory tendency. As discussed above, under the given Internet environment, a co-regulatory approach to Internet content regulation is essential. The South Korean government should not ignore this trend in order to ensure its regulatory effectiveness on the Internet.

Secondly, the Internet industry is required to develop codes of conduct, in order to ensure that it acts in accordance with its social *responsibility*. As mentioned above it is a prime example that the Korea Game Industry Alliance (KGIA) developed its code of conduct in 2002. In this context, the codes of conduct critically need to be of benefit not only to the industry itself, but also to the general public.

Thirdly, all the parties who are involved in the regulatory system, ranging from the government to civil organisations and individual Internet users, need to make considerable efforts to *reinforce* end-users' cyber-literacy. This goal would be achieved through continuous education and awareness campaigns. The EU 'Action Plan on Promoting Safer Use of the Internet' has allocated 46 percent of its total budget for encouraging awareness actions during its second phase (European Commission, 2003a). The government and ICEC need to make a significant effort into promoting awareness campaigns rather than to monitor and deliberate controversial information on the Internet. In my view, it would be the best solution to deal with problematic Internet contents in the long-term.

In sum, the above three points: *reforming* the government's Internet content regulation policy, ensuring the Internet industry's *responsibility* and *reinforcing* end-user's cyber-literacy are the essential elements which I have named the Korean R3 Net strategy. This strategy is based on the principles of

the EU Action Plan: co-operation, self-regulation and user empowerment, but I formulate it to take into account the unique regulatory environment in South Korea.

CHAPTER 10

CONCLUSION: THE FUTURE OF INTERNET CONTENT REGULATION

10.1. Introduction

As discussed in the previous chapter, just like in the real world there is a variety of evident dangers on the Internet, from expressions of hatred to child pornography. Of course, these problems are not limited to the Internet. Nevertheless they are often more complicated than the equivalent problems in the real world because of the unique characteristics of the Internet, such as globalisation, anonymity, synchronisation and a high degree of interaction. The European Commission (2003a) states, "New online technologies, new users and new usage patterns create new dangers and exacerbate existing dangers at the same time as opening a wealth of new opportunities." For this reason, it has been claimed that on the Internet a certain degree of regulation is inevitable. However, many libertarians argue for unlimited freedom of expression and object to any legal restrictions on the Internet. In 1996 John Barlow, a co-founder of the Electronic Frontier Foundation, announced *A Declaration of the Independence of Cyberspace*. He claimed that the Internet is naturally independent of any governmental control and people who create this global social space are forming their own social contract as follows:

> Your legal concepts of property, expression, identity, movement and context do not apply to us. They are based on matter. There is no matter here. [...] The only law that all our constituent cultures would generally recognise is the Golden Rule. We hope we will be able to build our particular solutions on that basis (Barlow, 1996b).

However, in my view, this utopian vision has failed, since the Internet has become increasingly commercialised in the 1990s (see Chapter 1: Footnote 4). The Internet is no longer a place only for good-willed experts any more. The population of the Internet is exploding. There are millions of newcomers who may not understand early Internet cultures which were built on "norms of

collaboration and cooperation." (Rheingold, 2000, p. 364) Unfortunately, it is evident that some of the Internet population are using the Internet for rather unpleasant purposes, for instance propagating hatred, distributing child pornography, selling pirated goods and infringing others' privacy.

Some libertarians claim that dangers on the Internet have been exaggerated, since the actual amount of problematic content, such as hate speech and child pornography is extremely small as compared to the enormous amount of information which is available on the Internet. Karin Spaink[1] wrote in her article, *From Quill to Cursor*, as follows:

> For instance, in 2000 Hatewatch.org counted between 450 and 500 'hard core' hate sites and circa 1750 sites that it deemed 'problematic.' Let's be very pessimistic and set the number at 50,000 pages all in all. Let's then set the amount of all existing pages in 2000 at 1 billion, a rather higher number. Basic maths tells us that even with these exaggerated figures 'hate pages' make up a mere 0.05 per cent of the total amount of pages (Spaink, 2003, p. 23).

However, I doubt whether the degree of danger can be assessed by these statistics. The above figure does not necessarily say that the number of problematic sites correlates with the degree of danger from them — in my view, what we need to watch carefully is to what extent these sites exercise an influence. The Internet is largely a reflection of the real world. Felipe Rodriquez said as follows:

> The anarchist cookbooks[2] are there, and so are the holocaust

---

[1] Karin Spaink is the chair of the Bits of Freedom (http://www.bof.nl), the main organisation for civil rights on-line in the Netherlands.

[2] The Anarchist Cookbook, which contains recipes for home-made bombs and engages in many other illegal and destructive activities, was originally written by William Powell in 1968 and 1969, during the Vietnam War, and was first published in 1971. Since then, hundreds of

> revisionists and consumers of bestiality. The availability of such content is a consequence of living in a global information and communications environment (Rodriquez, 2003, p. 107).

It cannot be expected that the marketplace of ideas works efficiently on the Internet, just as it hardly works in the real world, although I still believe that the Internet has potential for revitalising grass-roots democracy – through the case studies in Chapter 8, I confirmed that the Internet has enabled social minorities to voice their concerns and to build their own communities in a cheap and convenient manner. The Internet has provided them with great opportunities which they never had in the real society (see Chapters 8.2 and 8.3). Furthermore, as mentioned in Chapter 6, in South Korea the Internet has exercised significant social and political power (see Chapter 6.1). As our society has been subject to a degree of regulation, cyberspace is also being subject to certain legal frameworks. In 1996 a proposal of the UK Internet industry, *R3 Safety-Net*, claimed "the Internet is not a Legal Vacuum." It states as follows:

> In general, the law applies to activities on the Internet as it does to activity not on the Internet. If something is illegal "off-line" it will also be illegal "on-line," and vice versa. [...] the law can be upheld on-line as well as off-line (ISPA UK, LINX & the Safe-Net Foundation, 1996).

Therefore, now "the question is not whether we will have regulation; it is what kind of regulation we will have." (Sunstein, 2001, p. 128) In reality many governments and Internet industries from the EU and the US to Singapore and China have attempted to regulate the Internet in various ways, regardless of

---

copycat publications, some with remarkably similar titles such as Anarchist Cookbook II, have been produced. The book is still available from most major bookshops, including Amazon.co.uk. Free downloading of text files of the book is available via the Website, http://www.anarchist-cookbook.com/ (Retrieved October 10, 2003).

whether their regulations are working properly.

10.2. A Critique of the Governmental Internet Content Regulation

In Chapter 2, I critically appraised intense debates over freedom of expression and governmental regulation on the Internet through six key case studies; *the Communications Decency Act* (CDA), *the Child Online Protection Act* (COPA) in the US, *the Broadcasting Services Act* in Australia, a series of Internet Regulations in China from 1996 to 2000, and the co-regulatory model in the UK and the EU. Through these case studies it was established that there are a variety of different approaches to Internet content regulation from nation to nation, although these governmental regulations have appeared to have limited power regarding Internet content. In some cases they rather have raised controversial censorship issues.

As an extreme example, the Chinese government has a serious concern about uncontrolled information through the Internet which may undermine its sovereignty and social order, as well as its cultural values. Internet regulation in China has been introduced primarily for political reasons whereas in Western countries the most widespread justification for Internet regulation is the protection of minors from illegal and harmful information. Thus, the regulation is based on the idea that the government should monitor and control information on the Internet.

The US, where the Internet was born, is another prime example. The US government has introduced a series of Internet content regulations, from the CDA in 1996 and the COPA in 1998 to the CIPA in 2000. These regulatory attempts have faced strong challenges from civil organisations, such as the ACLU and the ALA. The US Supreme Court has also upheld civil

organisations' viewpoint and repeatedly ruled them unconstitutional. In these legal battles, one thing which was significant was that the US Court recognised the Internet as a print-like rather than a broadcast-like medium. In the CDA case, which was the first court case concerning Internet content regulation, the Court concluded that the Internet should enjoy freedom of expression just as the print media do, since "the Internet has achieved, and continues to achieve, the most participatory marketplace of mass speech that this country — and indeed the world — has yet seen." (*ACLU v. Reno* 929 F. Supp. 824, 1996) Thus, it cannot be regulated in the same way that broadcast media is regulated. The information available on the Internet should be treated like the information available in books and magazines, not like that in broadcast media. The European Union's perspective is similar to this. On its four-year work program, *A Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combatting Illegal and Harmful Content on Global Network*, it states that:

> Information on the Internet should be allowed the same free flow as paper-based information. Any restrictions should respect fundamental rights such as freedom of expression and the right to privacy (European Commission, 1999b).

However, unlike the US Supreme Court's viewpoint, the Australian government has recognised the Internet as a broadcast-like medium. In Australia, Internet content has been regulated by the Australian Broadcasting Authority (ABA) and the Office of Film and Literature Classification (OFLC). These two institutions are playing major roles in the regulation of radio wave and digital broadcast, and in rating of publications, movies and computer games respectively. Therefore, it can be said that the Australian Internet content regulation is based on the governmental content classification system, including the age classification system, which is applied to existing traditional media. For these reasons many libertarians and civil organisations, such as the

Electronic Frontiers Australia (EFA), claim that the legislation promotes censorship.

At this point, we need to discuss what kind of regulatory model would be applied to the Internet medium. The European Union and the US Supreme Court's viewpoints say that Information on the Internet should be treated in the same way as information in the print media in order to maximise freedom of expression on the most participatory and interactive medium, the Internet. However, this does not mean that the regulatory model of print media is good enough to regulate the Internet. The Internet is a truly complex medium. The Internet works as both a print medium as well as a broadcast medium. Although it has characteristics of both print and broadcast media, it can be defined neither as a broadcast medium nor as a print medium. There is no dichotomy. It has integrated all kinds of human communication technologies into itself and has become the first all-round global human communication medium spanning everything from personal communication, such as mail and telephone, to mass public communication areas, including newspapers, radio, television and so on.

Therefore, it can be argued that an old regulatory paradigm which has been applied to traditional media may be inadequate to cover the Internet medium where new integrated communication technologies are emerging. Thus, a new paradigm of Internet content regulation is ultimately required. In reality, as discussed, many direct governmental Internet regulations have faced various challenges, largely because the governments failed to recognise the unique characteristics of the new medium and then inappropriately applied the old paradigm of content regulation to the Internet which has a decentralised global architecture. After this, in European countries, the trend of Internet content regulation swiftly turned toward co-regulation which consists of five main

elements; Internet industry, self-rating and filtering, hotline (a voluntary reporting and complaints system), law enforcement and media-literacy. This co-operative model has been endorsed by many governments, including the European Union, as the most effective practice for dealing with harmful and illegal content on the Internet.

10.3. Is the Co-Regulatory Model a Right Answer?

Once again, it is important for us to be aware of the unique characteristics of the Internet medium for discussing a new regulatory model. First of all, the Internet is a global medium. Under this global architecture regulatory regimes worldwide have faced difficulties in exercising their own jurisdiction, while millions of Internet users have effortlessly cut across frontiers. A certain type of content or certain information which is illegal in one country is not necessarily illegal in other countries, because each nation has its own legal standard which reflects its social and political background. For instance, the criterion of harmful content differs in European nations. In the case of *Handyside v. the UK*,[3] Mr. Richard Handyside was prosecuted for possession of the Little Red Schoolbook which was circulated freely in other European countries (Akdeniz, 2001c).

At the same time, it is referred to as the most interactive and participatory medium. It provides truly bi-directional communication, because the difference between providers and recipients is not clear-cut on the Internet. In principle, all Internet users can be suppliers of content and not merely recipients, since the Internet allows various forms of interactive communication; from one-to-one and one-to-many communications to many-to-many communication (see

[3] see Chapter 2: Footnote 7.

Chapter 1: Footnote 8).

Moreover, it is still evolving in both technical and socio-economic aspects. As a prime example, Internet access speeds are increasing all the time. One of the most popular broadband technologies, Digital Subscribers Line (DSL), is still undergoing further development. Around the world, the number of broadband subscribers is growing rapidly, with a 72 percent increase during 2002 (ITU, 2003, p. 2). With this faster always-on Internet connection, the type and quantity of content on the Internet is drastically changing. In South Korea where over 93 percent of Internet subscribers use broadband, the Internet has strengthened its characteristics as a broadcast and entertainment medium. People can watch last week's soap operas and listen to live radio shows through VOD (Video-On-Demand) and Streaming services on the Internet. Several hundred page reference books and journals can be downloaded in Portable Document Format (PDF) in a matter of minutes. Downloading or exchanging of large files, even a one gigabytes movie file, is a common exercise of moderate broadband users. Indeed, the Internet which is becoming increasingly integrated into our daily life has not stopped growing yet. The Internet revolution has not finished.

These are the reasons that the Internet environment calls for a flexible and globally interpretable regulatory model rather than direct governmental regulation. In this sense, as discussed above, many Internet self-regulatory institutions across Europe, such as the Internet Watch Foundation UK, have adopted a co-operative model of regulation. The European Union has also endorsed this regulatory model under the 'Action Plan on Promoting Safer Use of the Internet.'

Although applauding its underlying aim; empowering end-users, I doubt

whether this co-operative regulation model is the right answer. The Action Plan is still in the process of development of the best practice model. It may be too early to judge its practical effects. Nevertheless, from the start it has been subjected to various criticisms.

10.3.1. Risk of Self-Regulation

The first point of criticism is regarding self-regulation of the Internet industry which works as one of the most important elements of the co-regulation model. Self-regulation of the Internet industry mainly focuses on dealing with harmful content on the Internet, but aids law enforcement agencies against illegal content and activities on the Internet through its hotline function. Spaink (2003, p. 21) argues that self-regulation is not able to "solve the fundamental problems" on the Internet, but raises privatised censorship issues as follows:

> [...] governments are privatising censorship, without assuming responsibility and accountability for it themselves, and without offering legal redress for either those censored or for those robbed of access to the censored content (p. 23).

Self-regulation of the Internet industry may raise a private censorship issue. However, self-regulation has not been designated to solve the fundamental issues related to Internet content. In terms of Internet content regulation it is only an option to deal with harmful content and to aid law enforcement agencies. As discussed in Chapter 3, lack of public accountability, ineffectiveness of enforcement and restricting competition have been the main grounds for criticism. Although it has previously been argued here that these criticisms are not a necessary feature of self-regulation, because most self-regulatory bodies are subject to control and scrutiny by government or other independent institutions, there is always a certain degree of risk of a self-

regulatory regime misusing its power which is delegated by the government.

10.3.2. Limitation of International Consent

The second point of criticism is that achieving international consent about illegal and harmful content is very difficult.

There are a few supranational and International agreements about certain types of illegal content, in particular child pornography. In May 2000, the UN General Assembly adopted 'the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography' (see Chapter 2: Footnote 22). In 2001 the Council of Europe (2001a) introduced the Convention on Cybercrime which articulates offences related to child pornography in its Article 9. In the same year the EU adopted the Council Framework Decision on combating the sexual expolitation of children and child pornography (European Commission, 2001b). As regards racism and xenophobia, the European Council issued a proposal for Council Framework Decision on combating racism and xenophobia which aims at prohibiting speech related to racism and xenophobia in EU Member States by criminal penalties (European Commission, 2002).

Despite these agreements, there are certain grey areas. For instance, as discussed in Chapter 2.4.2, while neo-Nazi propaganda is illegal in Germany, the Netherlands and some other European countries, it is constitutionally protected in the US. So far, child pornography is the only one category which is undoubtedly illegal worldwide — a number of international operations against Internet child pornography networks have already been launched, such as Operation Hamlet in 2002 (see Chapter 3.6.1.3). However, even the laws regarding child pornography differ nation by nation. While the simple

possession of child pornography is a criminal offence in the UK, it is not an offence in Sweden (Akdeniz, 2000). Indeed, the differences between nations' legal standards make the area of global co-operation even more limited. Moreover, in the case of harmful information the problem is much more serious. The meaning of 'harmful content' is completely different nation by nation. It is simply impossible to bring any consent to harmful information beyond a national level. Charlesworth (2000, p. 61) argued:

> The terminology in the Action Plan is regrettably vague about just what exactly is nature of the material to be addressed by the various initiatives. It makes a distinction between 'harmful' and 'illegal' content, stating the two types of material should be treated differently, but then fails to provide a workable definition of either.

10.3.3. Defect of Technical Solutions

The third point of criticism is about technical solutions that are employed for dealing with information which is deemed harmful, but not strictly illegal.

As discussed in Chapter 4 no commercial filtering software, the so-called first generation filtering products, is free from its inherent shortcomings. Rather, it gives parents and teachers a false sense of security as most commercial filtering product companies provide scant information about the product's inherent technical limitations, whereas they are quick to advertise how brilliant their products are. "A danger of [these commercial filtering products] is that once a filter system has been installed, parents and teachers, believing that their children are now in a safe environment, will see no need for further supervision." (Economic and Social Committee of the European Commission, 1998) These kinds of filtering products may be useful in a primary school classroom. At most general public Internet access points, for instance public

libraries and Internet cafés, however, they may work as a privatised censorship tool rather than as an effective solution to prevent minors from accessing harmful information. In my view, usage of commercial filtering software would be restricted to a few very limited environments.

Another technical solution, the Internet content rating system, has similar problems. First of all, its filtering coverage is very narrow. It works only on the World Wide Web, while FTP, newsgroups, peer-to-peer and many other communication models are beyond its scope. Furthermore, it has not yet taken its practical effect. It has been four years since ICRA launched with project funding of the Action Plan. However, its popularity, including the number of rated Websites, is not at all impressive despite the fact that its success largely depends on this. I very much doubt whether any Internet content rating system is able to reach its critical mass in the foreseeable future, since the system relies largely on uncompensated participation of millions of Internet users and information providers. In this sense, it is argued that the Internet content rating system cannot be operational without the threat of meaningful sanctions.

In practice, the South Korean government introduced its mandatory Internet content rating system in the name of minor protection from inappropriate information on the Internet. However, this mandatory rating system has raised many controversial censorship issues. Through the case study of the mandatory Internet content rating system in South Korea, I can confirm the dangers of the mandatory rating system. It has restricted social minorities' voices and activities on the Internet. Indeed, it has been used as a governmental censorship tool rather than an optimal technical solution for self-regulation on the Internet. In this context, I argue that there are possibilities that any developing nation worldwide may employ the Internet content rating system as a censorship tool.

10.3.4. Recommendations

In sum, the current European co-operative regulation model is not yet satisfactory. In my view, it still has great potential in terms of user empowerment. For the further development of this regulatory model, the following recommendations would be discussed.

Firstly, the Internet industry should provide transparency of its activities in this regulatory model and make an effort to obtain public credibility. For instance, it may achieve this goal through joint actions with civil liberties organisations. Secondly, it is recommended that any government or self-regulatory regime would not endorse usage of commercial filtering software. It is simply inadequate that the co-operative regulatory model employs filtering software which has such inherent weaknesses (see Chapter 4.4). Thirdly, just like the first generation filtering software, adopting the Internet content rating system should be fundamentally reconsidered. As discussed, the practicality of implementation is doubtful. Through the case study of the South Korean Internet content rating system, we saw the potential risk of the system is being employed as a tool for governmental censorship (see Chapter 7.3). Furthermore, ICRA's standalone filtering software, ICRA*filter* supports blacklist based filtering. Its latest software, ICRA*plus* employs even more controversial technologies, such as artificial intelligence agents and image recognition technologies. These features may raise contentious issues concerning end-users' autonomy and freedom of expression. Finally, in the long term this model should focus on empowering end-users through reinforcing its awareness actions. The European Union already seems to be on the right track, since the second phase of the Action Plan has earmarked 46 percent of its total budget for encouraging awareness actions.

10.4. The Future of Internet Content Regulation

> The debate about online content is still very much alive, and none of the available solutions to protect against offensive content are completely satisfactory (Rodriquez, 2003, p. 86).

The debate over the Internet content regulation is still a contentious ongoing issue. Although there are many different viewpoints on this issue, the main trend of Internet content regulation in European nations has shifted from direct governmental regulation towards co-regulation. So far, none of these regulatory models are satisfactory for everyone.

On the Internet, much information comes from outside jurisdiction, since "the cost and speed of information transmission on the Internet is almost entirely independent of physical location." (Johnson & Post, 1996) Consequently it reflects very different moral, religious and political standards. Certain information which is illegal in one country is not necessarily illegal in other countries. From end-users' standpoint, ultimately, adult end-users have the right to access any information they wish to see, as long as the information is not illegal in jurisdiction of access point, regardless of whether the Information is legal or illegal in jurisdiction where it is physically stored. The first responsibility of information on the Internet is placed on Internet users themselves who create, distribute and use it. Controlling their children's activities on the Internet is also up to them. Indeed, Internet users constitute the main body to develop and regulate the Internet. However, in reality we cannot shift all the responsibility for illegal and harmful information on to them. The Internet is neither a smooth-running marketplace of information nor a utopian idyll where all users are people of goodwill.

Through the study it was found that collective efforts of all parties from

governments to civil organisations are absolutely needed to tackle the issue concerning illegal and harmful information on the Internet. Although the European Union's regulatory model is not completely adequate, it has given us three key concepts for the future of Internet content regulation: co-operation, self-regulation and user empowerment. Based on these principles I formulated the Korean R3 Net strategy which incorporates the following three points: *reforming* the government's Internet content regulation policy: ensuring the Internet industry's *responsibility* and *reinforcing* end-user's cyber-literacy (see Chapter 9.7).

Taking into account the experiences of Internet content regulation in Europe and South Korea, I have drawn the following diagram which shows a collective regulatory model. It consists of the participation of the following four parties: the Internet Industry, government, civil organisations and end-users:

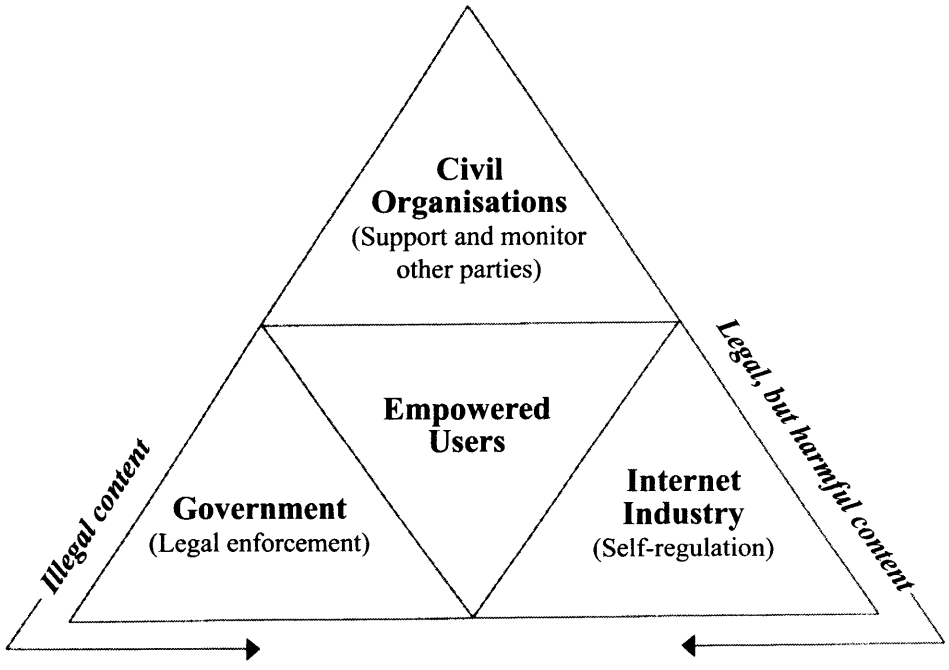

Fig. 10.1. A collective regulatory model

After all, the basic idea behind this model is that all interested parties would jointly devote their efforts to empower end-users. Furthermore, this regulatory system aims to force all three parties, the government, the Internet industry and civil organisations, to equally share power and to monitor each other in order to ensure credibility of the regulatory system and to prevent misuse of regulatory power.

As discussed through the study of the South Korean government's Internet content regulation, there is a possibility that the government would tend to excessively regulate controversial Internet content in the name of child protection or national security. Therefore, external consultation and monitoring of the governmental regulatory agencies are crucial to prevent them from arbitrarily exercising their regulatory power. In this context, civil organisations have an important role to monitor not only the governmental agencies' regulatory practice, but also self-regulation of the Internet industry.

In the existing co-regulatory model, many actions are conducted by industry-based institutions with governmental support. However, this study identified that some of these actions are not satisfactory, because they have a number of problems related to issues of public accountability and transparency. In this context, this model does not give support to industry-based hotline reporting systems. However, it does not mean that it denies the role of hotline systems in the Internet content regulation system, in particular related to illegal content. As discussed in Chapter 3, industry-based hotlines have been criticised for being "self-appointed judges of law" (ACLU, 1999c). A survey, *Eurobarometer: Illegal and harmful Content on the Internet* (European Commission, 2004b, p. 32), highlighted the "lack of information of the European Union citizens about where or whom to report illegal or harmful content on the Internet." While 38 percent of the respondents admitted they do

not know whom to address, 37 percent say they would go to the police. Only eight percent would address the Internet service provider and five percent would call hotlines. This result indicates that the public recognition of industry-based hotlines is far too low. In order to ensure the popularity of hotline systems, as well as accountability, transparency and democracy, they need to turn into a collaborative body.

Alongside the call for a collaborative body's hotline system, this model excludes technical solutions, such as Internet content filtering and rating systems. As mentioned, these technical solutions have inherent weaknesses and allow the possibility of upstream filtering which may threaten end-users' autonomy and rights to freedom of expression (see Chapters 4 and 5). I have no objection to parents deciding to use commercial filtering software at home for their own children, as long as they are aware of its limitations. However, in my view, parental advice about safer use of the Internet should be emphasized rather than use of these technical solutions. At home, time schedule-based Internet access controlling, which is available in most commercial filtering software, would be an alternative to blacklist or keyword based filtering (see Chapter 4.3.2). Apart from the personal usage, these technical solutions should be prohibited at public Internet access points, in particular PC cafés and public libraries — in South Korea PC cafés must install such Internet content filtering software by law (see Chapter 7.2).

Another issue that needs to be clarified in this regulatory model is a distinction between illegal and harmful content. As discussed repeatedly, illegal content and harmful content are significantly different issues in nature. When the distinction is blurred, freedom of expression can be restricted. ICEC is a prime example; it had not clearly distinguished illegal and harmful content in its deliberation procedure, but had excessively restricted a number of Websites

which contained controversial information or ideas under the vague regulatory concept, named "improper communication" until the Constitutional Court held it to be unconstitutional (see Chapter 9.2). The government holds a primary responsibility for regulating illegal content and activities on the Internet. Self-regulation is only secondary as regards illegal content. The management and control of harmful content is in principle an issue of user and consumer choice and responsible industry practices (Pierlot, 2000).

Based on these principles each party in this model should work as follows: Firstly, the Internet industry should make self-regulatory efforts, such as developing codes of conduct, in order to promote its public accountability and transparency. Secondly, the government should support self-regulatory activities of civil organisations and the Internet industry, while it should enforce legislation to deal with illegal content and activities on the Internet. Thirdly, civil organisations should support and monitor other parties in order to ensure that they act in accordance with their social responsibility.

For this collective regulatory model the following actions should be taken:

Encouraging credible self-regulation: In order to ensure credibility of self-regulation, as Akdeniz (2005) argues, the Internet industry should adopt codes of conduct which guarantee external consultation and involvement of all concerned parties, including consumer, public interest and other independent representatives, in its self-regulatory bodies and practice. The code should also include "clear and intelligible statements of principle and measurable standards [...] which address real consumer and user concerns." Under the codes of conduct, the self-regulatory scheme should "identify the intended outcomes." Furthermore, it should be "well publicised with maximum education and information directed at consumers and users" and "regularly reviewed and

updated in the light of changing circumstances and expectations" (Akdeniz, 2005). In addition, the government should provide self-regulatory bodies with legal and administrative support. The role of the government is decisive in establishing and managing a credible self-regulatory scheme. On the one hand, without the governmental support the self-regulatory scheme cannot secure its enforcement power. On the other hand, the government is able to effectively redress abuses of self-regulatory power. As mentioned previously, "self-regulation works best within a legal framework." (National Consumer Council, 2000, p. 48).

Providing collaborative institutional measures: Collaborative institutional measures for ensuring end-users' participation, such as hotline reporting systems and watchdog groups, would be developed and provided. In this sense, monitoring of the existing industry-based hotlines' actions should be available to the public. In the long term, it is recommended that the main body of hotline systems should be a collaborative body which includes various concerned parties rather than the industry alone.

Raising awareness: Through awareness education and campaigns at both national and international levels the public's Internet literacy should be enhanced. Developing educational materials and publications about safer Internet use is required. The best method of delivery according to each target group, from primary school pupils to adults, should be researched. This awareness strategy has already been adopted by the European Union's Action Plan. According to a report from the Action Plan (European Commission, 2003b), there are a number of national and European awareness programmes. "Altogether 12 projects covering 16 [...] countries have taken part in projects establishing contacts and collaborative networks to raise awareness with partners from the public sector and NGOs and limited participation of

industry." 4.05 million EUR and 3.65 million EUR respectively were earmarked for the Action Plan's awareness action line in 2003 and 2004. However, as the report concedes, this amount of funding is too small to cover the huge potential target audience for awareness action. In my view, the Action Plan would concentrate its efforts on its awareness action line, while other action lines, such as developing filtering and rating system, should be reconsidered. The awareness action may not come to fruition in a short term. However, I believe that it would be the best way to empower end-users in the long run.

In the Internet era, a sole government regulation cannot achieve its aim. Instead, at both national and international levels, all the concerned parties, from governments and the Internet industries to civil organisations and individual end-users, need to mutually co-operate in addressing issues over illegal and harmful content on the Internet. In this context, Akdeniz (2001a, p. 131) argues:

> [A] multi-layered approach to Internet governance is inevitable, one in which a mixture of public and private bodies will be involved, and which includes the individual Internet users, for control as far as harmful content is concerned. A multi-layered approach will also include layers at a supranational and international level of Internet governance.

Through a number of case studies, this thesis has identified that the government-centred regulation of Internet content in South Korea appears to be not only ineffective, but also faced with a number of censorship issues. As Hwang and Hwang (2003, p. 473) argue, in South Korea content regulation has been a matter for the government, but a co-regulatory scheme is essential in the Internet era. This argument is now being supported not only by civil organisations and academics, but also a governmental agency. In November

2004 the National Computerization Agency (NCA, 2004, pp. 14-16) published a report which proposes that a new Internet content policy should tend toward reforming regulatory agencies and legislations, encouraging non-governmental sectors' self-regulation and empowering end-users. Therefore, the question which remains to be answered is about finding an optimal co-regulatory model. What is the optimal co-operative Internet content regulatory model? How can we achieve it? I hope that the regulatory model I proposed above would be a step toward the future of the Internet content regulation. In my view "user empowerment" and "co-operation," the two core elements of this model, are the best solutions for Internet content regulation. One thing we should always bear in mind is that different models and approaches are needed for illegal and harmful content. While dissemination of illegal content should be regulated by law, harmful content falls within the protection area of the right to free speech. As the European Court of Human Rights has confirmed, freedom of expression is applicable not only to information or ideas that are favourably received or regarded as inoffensive, but also to those that offend, shock or disturb any category of people.[4] The goal of Internet content regulation is not to make the Internet an impeccable place, but a better and safer place where freedom of expression and regulation possibly strike a balance.

[4] The Case of *Handyside v. the UK* (1976) §49. see Chapter 2: Footnote 7.

BIBLIOGRAPHY

ABA (1997, October). The Internet and some international regulatory issues relating to content: A pilot comparative study commissioned by the UNESCO. Retrieved March 18, 2005, from http://www.aba.gov.au/internet/research/unesco/pdfrtf/unesco.pdf

ABA (2004). The ABA annual report 2003-2004. Retrieved March 5, 2005, from http://www.aba.gov.au/abanews/annRpt/an03-04/index.htm

ACLU (1997). Fahrenheit 451.2: Is cyberspace burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet. Retrieved February 7, 2002, from http://www.aclu.org/issues/cyber/burning.html

ACLU (1999a). Rejecting cyber-censorship, court defends online "marketplace of ideas." Retrieved May 2, 2003, from http://www.aclu.org/news/1999/n020199a.html

ACLU (1999b). Internet censorship battle moves to appeals court. Retrieved May 2, 2003, from http://archive.aclu.org/news/1999/n040299a.html

ACLU (1999c). ACLU joins international protest against global Internet censorship plans. Retrieved March 15, 2004, from http://archive.aclu.org/news/1999/n090999a.html

ACLU (2001). ACLU files challenge to library Internet censorship in case fast-tracked for Supreme Court review. Retrieved September 11, 2001, from http://www.aclu.org/features/f032001.html

Aguilar, Rose (1996). Site filters criticised. *CNet News*. Retrieved May 31, 2003, from http://news.com.com/2100-1023-239358.html?legacy=cnet

Ahlert, Christian, Marsden, Chris & Yung, Chester (2004, May). How 'Liberty' disappeared from cyberspace: The mystery shopper tests Internet content self-regulation. Programme in Comparative Media Law & Policy Centre for Socio-Legal Studies, University of Oxford. Retrieved March 22, 2005, from http://pcmlp.socleg.ox.ac.uk/liberty.pdf

Ahn, Chi-Yong (2001, June 19). CYBER 'MYONGDONG SEONGDANG' DEUNGJANG [The advent of cyber 'Myongdong Cathedral']. *KYOUNG-HYANG SHINMUN*. Retrieved April 6, 2005, from http://www.khan.co.kr/news/artview.html?artid=200106191956221&code=930100

Ahn, Dong-Geun (1999, June 26). JEONGBO TONGSING NAEYONG SIMUIUI BIPANJEOK BUNSEOK [Critical analysis of info-communication content deliberation]. The 3rd Academic Symposium. HANGUK JEONGBO BEOP HAKHOE. Seoul. Retrieved April 4, 2005, from http://www.kafil.or.kr/old_kafil/seminar/s3-adk.PDF

Ahn, Kyong-Whan (1997). The Influence of American Constitutionalism on South Korea. *Southern Illinois University Law Journal, 22*, 71-115.

Akdeniz, Yaman (1996). Computer pornography: a comparative study of the US and UK Obscenity laws and child pornography laws in relation to the Internet. *International Review of Law, Computers & Technology, 10(2)*, 235-261.

Akdeniz, Yaman (1997a). Governance of pornography and child pornography on the global Internet: A multi-layered approach. In Edwards, Lilian & Waelde, Charlotte (Eds.), *Law and the Internet: Regulating Cyberspace* (pp.223-241). Oxford: Hart Publishing.

Akdeniz, Yaman (1997b) The regulation of pornography and child pornography on the Internet. *Journal of Information, Law & Technology 1997(1).* Retrieved March 12, 2005, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz1/

Akdeniz, Yaman (1999). *Sex on the net: The dilemma of policing cyberspace.* Reading, England: South Street Press.

Akdeniz, Yaman (2000). Child pornography. In Akdeniz, Yaman, Walker, Clive & Wall, David (Eds.), *The Internet, law and society* (pp. 231-248). Essex, England: Pearson Education Limited.

Akdeniz, Yaman (2001a). Controlling illegal and harmful content on the Internet. In Wall, David S. (Ed.), *Crime and the Internet* (pp. 113-140). London: Routledge.

Akdeniz, Yaman (2001b) Governing pornography & child pornography on the Internet: The UK approach. In Cyber-Rights, Protection and Markets: A Symposium. University of West Los Angeles Law Review, 247-275.

Akdeniz, Yaman (2001c). Internet content regulation: UK government and the control of Internet content. *Computer Law & Security Report, 17(5)*, 303-317.

Akdeniz, Yaman (2003). Regulation of Child Pornography on the Internet: Cases and Materials. Retrieved March 12, 2005, from http://www.cyber-rights.org/reports/child.htm.

Akdeniz, Yaman (2004). Who watches the watchmen? The role of filtering software in Internet content regulation. In OSCE (Ed.), *The media freedom Internet cookbook* (pp. 101-121). Vienna: OSCE.

Akdeniz, Yaman (2005, February 4). Controlling Internet Content: Implications for Cyber-Speech. In International Conference on Freedom of Expression in Cyberspace. UNESCO, Paris. Retrieved April 05, 2005, from http://www.cyber-rights.org/paris_ya.pdf

Akdeniz, Yaman & Strossen, Nadine (2000). Sexually orientated expression. In Akdeniz, Yaman, Walker, Clive & Wall, David (Eds.), *The Internet, law and society* (pp. 207-230). Essex, England: Pearson Education Limited.

Akdeniz, Yaman, Walker, Clive & Wall, David (Eds.) (2000) *The Internet, law and society*. Essex, England: Pearson Education Limited.

ALA (2001). American library association files lawsuit challenging children's Internet Protection Act. Retrieved January 25, 2002, from http://www.ala.org/cipa/cipapressrelease.html

ALA (2002). ALA presents arguments in first day of CIPA challenge. Retrieved June 14, 2004, from http://www.ala.org/pressreleasesbucket/alapresentsarguments.htm

ALA (2003). ALA reaffirms core values, commitment to members at August 23 meeting: A statement from ALA President Carla Hayden. Retrieved June 14, 2004, from http://www.ala.org/ala/pressreleasesbucket/pressreleases2003aug/statementala.htm

ALA Intellectual Freedom Committee (2000). Statement on library use of filtering software. Retrieved October 31, 2001, from http://www.ala.org/alaorg/oif/filt_stm.html

ALA Washington Office (1996). Library Services and Technology Act: Basic questions and answers. Retrieved November 1, 2001, from http://www.ala.org/washoff/lstaqa.html

Archer, Phil (2004). ICRA's experience of the technical and policy issues related to content labelling. Retrieved June 15, 2004, from ICRA Website: http://www.icra.org/press/www2004/www2004.pdf

Attorney General's Commission on Pornography. (1986). *Attorney General's Commission on Pornography: Final report.* Washington, DC: US Government Printing Office.

Baek, Uk-In (2001). DANGSINDEULIYAMALRO EUMRANHADA: KIM IN-KYU GYOSAREUL YONGHOHAMYEO [You are obscene: Supporting Kim In-kyu the teacher]. *GYOYUK BIPYEONG, 5*, 258-267.

Baldwin, Robert & Cave, Martin (1999). *Understanding regulation.* Oxford: Oxford University Press.

Balkin, M. J., Noveck, Beth & Roosevelt, Kermit (2000). Filtering the Internet: A best practices model. In Waltermann, Jens & Machill, Marcel (Eds.), *Protecting our children on the Internet* (pp. 199–261). Gűtersloh, Germany: Bertelsmann Foundation Publishers.

Bannan, Karen (2001). Clean it up. *PC Magazine*. Retrieved November 1, 2001, from http://www.pcmag.com/article/0,2997,s3D40026a3D12392,00.asp

Baran, Paul (1964). Distributed communications: I. Introduction to distributed communications networks. Retrieved June 22, 2004, from RAND Corporation Website: http://www.rand.org/publications/RM/RM3420/

Barbrook, Richard (1996). Hypermedia freedom. In Ludlow, Peter (Ed.). (2001), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 47-58). Cambridge, Massachusetts: MIT Press.

Barbrook, Richard & Cameron, Andy (1995). Californian ideology. In Ludlow, Peter (Ed.). (2001), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 363-387). Cambridge, Massachusetts: MIT Press.

Barendt, Eric (1985). *Freedom of Speech.* Oxford: Oxford University Press.

Barlow, John Perry (1996a, January 15). Thinking locally, acting globally. *TIME*. Retrieved July 5, 2004, from http://www.eff.org/Misc/Publications/John_Perry_Barlow/think_local_act_global_011596.article

Barlow, John Perry (1996b). A declaration of the independence of cyberspace. Retrieved March 31, 2001, from http://www.eff.org/~barlow/Declaration-Final.html

Barme, Geremie & Ye, San (1997, June). The great firewall of China. *Wired, 5.06*, pp. 138-151

Barton, Ben F. & Barton, Marthalee S. (1993). Modes of power in technical and professional visuals. *Journal of Business and Technical Communication, 7(1)*, 138-162.

BBC (2003, July 21). Hot topics: Artificial intelligence. Retrieved March 16, 2004, from http://www.bbc.co.uk/science/hottopics/ai/

Beom, Yong (2002a, June 1). JEONGTONGYUN 'GUNDAE BANDAE' HOMPAGE HAMGURYEONG [ICEC gives 'anti-army' homepage an order to keep silence]. *INGWON HARU SOSIK, 2106*. Retrieved April 3, 2005, from http://www.sarangbang.or.kr/

Beom, Yong (2002b, June 4). 'GUNDAE BANDAE' HOMEPAGE GYEOLGUK PYAESWAE ['Anti-army' hompage finally closed down]. *INGWON HARU SOSIK, 2107*. Retrieved April 3, 2005, from http://www.sarangbang.or.kr/

Bender, Gunnar (1998). Bavaria v. Felix Somm: The pornography conviction of the former CompuServe manager. *International Journal of Communications Law and Policy, Web-Doc 14-1-98*. Retrieved March 22, 2005, from http://www.ijclp.org/1_1998/ijclp_webdoc_14_1_1998.html

Bennahum, David S. (1996). United nodes of Internet: Are we forming a digital nation? In Ludlow, Peter (Ed.). (2001), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 39-45). Cambridge, Massachusetts: MIT Press.

Better Regulation Task Force (1998, September). Annual Report 1997-1998. Retrieved March 22, 2005, from http://www.brtf.gov.uk/docs/pdf/a_report98.pdf

Better Regulation Task Force (1999, October). Self-regulation: Interim report. Retrieved March 19, 2005, from http://www.brtf.gov.uk/docs/pdf/self_regulation.pdf

Black, Julia (1996). Constitutionalising self-regulation. *The Modern Law Review*, 59, 24-55.

Bowman, Lisa (2001). Lawsuits slam Net filtering efforts. *CNet News*. Retrieved September 10, 2001, from http://news.cnet.com/news/0-1005-200-5196773.html

Boyle, James (1997). Foucault in cyberspace: Surveillance, sovereignty, and hard-wired censors. *University of Cincinnati Law Review*, *66*, 177. Retrieved March 10, 2004, from http://www.law.duke.edu/boylesite/foucault.htm

Brin, David (1997). Getting our priorities straight. In Ludlow, Peter (Ed.). (2001), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 31-38). Cambridge, Massachusetts: MIT Press.

Breyer, Stephen (1982). Regulation and its reform. Cambridge, Massachusetts: Harvard University Press.

Cabinet Office (1999, September). e-commerce@its.best.uk. Retrieved March 29, 2005, from http://www.number-10.gov.uk/su/ecomm/ec_body.pdf

Campbell, Angela J. (1999). Self-regulation and the media. *Federal Communications Law Journal*, *51(3)*, 711-772.

Cannataci, Joseph A. & Bonnici, Jeanne P. M. (2002, April). Can self-regulation satisfy the transnational requisite of successful Internet regulation? In 17th BILETA Annual Conference. Amsterdam. Retrieved March 19, 2005, from http://www.bileta.ac.uk/02papers/cannataci.html

Castells, Manuel (2001). *The Internet galaxy: Reflections on the Internet, business, and society.* New York: Oxford University Press.

Castells, Manuel (2004). *The information age: Economy, society and culture vol. 2: The power of identity* (2nd ed.). Oxford: Blackwell Publishing.

Censorware Project (2000). Loudoun County, VA Censorware Lawsuit. Retrieved March 26, 2005, from http://censorware.net/legal/loudoun/

Center for Democracy and Technology (1999). An analysis of the Bertelsmann Foundation memorandum on self-regulation of Internet content: Concerns from a user empowerment perspective. Retrieved March 14, 2004, from http://www.cdt.org/speech/991021bertelsmannmemo.shtml

Cerf, Vint (1994, August 14). Guidelines for conduct on and use of Internet (Draft v0.1). Retrieved March 16, 2005, from http://www.isoc.org/internet/conduct/cerf-Aug-draft.shtml

Charlesworth, Andrew (2000). The governance of the Internet in Europe. In Akdeniz, Yaman, Walker, Clive & Wall, David (Eds.), *The Internet, law and society* (pp. 47-78). Essex, England: Pearson Education Limited.

Chase, Michael S. & Mulvenon, James C. (2002). You've got dissent! Chinese dissident use of the Internet and Beijing's counter-strategies. RAND. Retrieved March 7, 2005, from http://www.rand.org/publications/MR/MR1543/

Cho, Kuk (2003). EUMRANMUL DDONEUN PORNOGRAPHY SOGO [Obscenity or Pornography Revisited]. *BEOPHAK*, 44(4), 141-162.

Cho, Kye-Wan (2000, June, 26). GEOMYEOL YURYEONGI ONLINE DEOPCHINDA [The ghost of censorship is coming online]. *The HANKYOREH21*. Retrieved July 14, 2002, from http://www.hani.co.kr/section-21010000/2000/02101000020000726031905 2.html

Chong, Jong-Sup (1999). HANGUKUI MINJUHWAE ISSEOSEO HEONBEOPJEPANSOWA GIBONGWONUI HYEOSIL: 1988NYEONBUTEO 1999NYEONGGKJI [The Constitutional Court and the attainment of fundamental rights in the democratisation of Korea: 1988-1998]. *BEOPHAK*, 40(3), 226-253.

Cincotta, Harward (Ed.). (1994). An outline of American history. Retrieved June 3, 2004, from the US Information Agency Website: http://usinfo.state.gov/products/pubs/history/toc.htm

Claburn, Thomas (2005, March 18). Firefox Eats More Microsoft Market Share. *InformationWeek*. Retrieved March 28, 2005, from http://www.informationweek.com/story/showArticle.jhtml?articleID=159902316

Clausing, Jeri (1998). In rejecting dismissal of filtering case, judge sets high standard for libraries. *The New York Times*. Retrieved May 19, 2003, from http://www.nytimes.com/library/tech/98/04/cyber/articles/09library.html

Consumer Reports (2001, March). Digital chaperones for kids. Retrieved November 25, 2001, from http://www.consumerreports.org/Special/ConsumerInterest/Reports/0103fil0.html

Commission for Racial Equality (2001). Race relations Act. Retrieved January 11, 2002, from http://www.cre.gov.uk/legaladv/rra.html

Commission on Child Online Protection (2000, October 20). Final Report of the COPA Commission. Retrieved June 16, 2004, from http://www.copacommission.org/report/COPAreport.pdf

Committee on Civil Liberties and Internal Affairs (1997, March 20). Report on the Commission communication on illegal and harmful content on the Internet. Rapporteur: PRADIER Pierre. PE219.568. Retrieved March 12, 2005, from http://www.europarl.eu.int/plenary/default_en.htm

Constitutional Court of Korea (2003). *Decisions of the Korean Constitutional Court*. Seoul: The Constitutional Court. Retrieved April 7, 2005, from http://www.ccourt.go.kr/english/download/decision_2003.pdf

Council of Europe (2001a). Convention on Cybercrime. European Treaty Series No. 185. 23 November 2001, Budapest. Retrieved March 14, 2005, from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Council of Europe (2001b). Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content. Retrieved January 5, 2002, from http://cm.coe.int/ta/rec/2001/2001r8.htm

Cullen, Richard & Choy, Pinky D. W. (1999). The Internet in China. *Columbia Journal of Asian Law, 13(1)*, 99-134.

Cyber-Rights & Cyber-Liberties (UK) (1997, November). Who watches the watchmen: Internet content rating systems, and privatised censorship. Retrieved March 14, 2004, from http://www.cyber-rights.org/watchmen.htm

Cyber-Rights & Cyber-Liberties (UK) (1998, September). Who watches the watchmen: Part II: Accountability & effective self-regulation in the information age. Retrieved March 27, 2005, from http://www.cyber-rights.org/watchmen-ii.htm

Cyveillance (2000). Internet exceeds 2 billion pages. Retrieved January 26, 2002, from http://www.cyveillance.com/newsroom/pressr/000710.asp

Darlington, Roger (2004). Should the Internet be regulated? Retrieved June 24, 2004, from http://www.rogerdarlington.co.uk/regulation.html

Das, Arun Kristian & Pike, Sarah (2001). Federally funded peep shows: The legal wrangling over CIPA. *PC Magazine*. Retrieved July 6, 2004, from http://www.pcmag.com/article2/0,1759,2846,00.asp

Delacourt, John (1997). The International impact of Internet regulation. *Harvard International Law Journal, 38*, 207.

Dertouzos, Micheal (1997). *What will be: How the new world of information will change our lives*. London: Piatkus.

Directorate General of Human Rights (2000). Case-law concerning Article 10 of the European Convention on Human Rights: 50th anniversary of the European Convention on Human Rights 1950-2000. Strasbourg. Retrieved February 21, 2005, from http://www.humanrights.coe.int/media/documents/dh-mm/caselaw-english.doc

Dixon, Ruth (2001, November 28). Co-operative forms of regulating the Internet. In Livingstone, Sonia (Chair), European Forum on Harmful and Illegal Cyber Content, Strasbourg, France. Retrieved January 23, 2002, from http://www.humanrights.coe.int/media/cyberforum/rep-dixon.rtf

Dixon, Ruth (2002). The Internet: A menace to society? In Cummings, Dolan (Ed.), *The Internet: Brave New World?* (pp.39-52) London: Hodder & Stoughton.

Dyson, Esther (1998). *Release 2.1*. New York: Broadway Books.

Economic and Social Committee of the European Commission (1998, April). Opinion on the proposal for a council decision adopting a multiannual community action plan on promoting safe use of the Internet. *Official Journal of the European Communities, C 214*, 29-32

Edelman, Benjamin (2001). Expert report of Benjamin Edelman: Multnomah County public library et al., vs. United States of America, et al. Retrieved December 12, 2001, from http://cyber.law.harvard.edu/people/edelman/pubs/aclu-101501.pdf

Edwards, Lilian (2000). Pornography and the Internet. In Edwards, Lilian & Waelde, Charlotte (Eds.), *Law and the Internet: A framework for electronic commerce* (2nd ed.) (pp. 275-308). Oxford: Hart Publishing.

EFA (2002a). Internet Censorship in Australia. Retrieved March 26, 2005, from http://www.efa.org.au/Issues/Censor/cens1.html

EFA (2002b). Review of the operation of schedule 5 to the Broadcasting Services Act 1992. Retrieved March 10, 2004, from http://www.efa.org.au/Publish/efasubm_bsa2002.html

Elmer-Dewitt, Philip (1995, July 3) On a screen near you. *TIME*, Vol. 146.

Engberg, David (1996). The virtual panopticon. Retrieved April 8, 2004, from http://is.gseis.ucla.edu/impact/f96/Projects/dengberg/

Euh, Yoon-Dae (1998). IMFUI WONINGWA DAEEUNGBANGAN [The cause and countermeasure of IMF]. *98 JEONGRYE HAKSUL BALPYO NONMUNJIP HANGUK MUYEOK HAKHOE*, 47-63.

EUMRANMUL JEOPGEUNEUN HEONBEOP BOHO YEONGYEOK BAK [Access to obscene materials does not fall within the protection area of the Constitution] (2004, February 2). *THE HANKYOREH SHINMUN*. Retrieved April 27, 2005, from http://www.hani.co.kr/section-005100030/2004/02/005100030200402020740045.html

European Commission (1996a, October 16). Green paper on the protection of minors and human dignity in audiovisual and information services (COM (96) 0483). Brussels. Retrieved June 12, 2004, from http://europa.eu.int/ISPO/infosoc/legreg/docs/protect.html

European Commission (1996b, October 16). Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Illegal and harmful content on the Internet (COM (96) 0487). Brussels. Retrieved June 12, 2004, from http://europa.eu.int/ISPO/legal/en/internet/communic.html

European Commission (1996c). Resolution on 'Europe and the global information society - Recommendations to the European Council' and on a communication from the Commission of the European Communities: 'Europe's way to the information society: an action plan' (COM(94)0347 - C4-0093/94). *The Official Journal of the European Commission, C 320* , 164.

European Commission (1997a). Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council of 17 February 1997 on illegal and harmful content on the Internet. *The Official Journal of the European Communities, C 070*, 1-2.

European Commission (1997b). Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 26 November 1997, Action Plan on promoting safe use of the Internet (COM(97)0582 Final). 26 November 1997.

European Commission (1999a). Action plan on promoting safer use of the Internet: Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. *The Official Journal of the European Communities, L33, Vol. 42*, 1-11.

European Commission (1999b). A multiannual community action plan on promoting safer use of the Internet by combatting illegal and harmful content on global networks; 4-year work programme 1999 – 2002. Retrieved October 12, 2003, from http://europa.eu.int/information_society/programmes/iap/docs/pdf/programmes/workprgm/work.pdf

European Commission (1999c). Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market. COM(98)0586 final. *The Official Journal of the European Communities, C30*, 4-35.

European Commission (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce'). *The Official Journal of the European Communities, L178,* 1-16.

European Commission (2001a). European governance: A white paper. COM(2001)428 final. Brussels. Retrieved March 23, 2005, http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0428en01.pdf

European Commission (2001b). Proposal for a council framework decision on combating the sexual exploitation of children and child pornography. COM(2000)845 final. *The Official Journal of the European Communities, C62*, 327-330.

European Commission (2002). Proposal for a council framework Decision on combating racism and xenophobia. COM(2001)664 final. *The Official Journal of the European Communities, C75*, 269-273.

European Commission (2003a). Decision No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. *The Official Journal of the European Union, L162, Vol. 46*, 1-4.

European Commission (2003b). Safer Internet action plan: Work programme 2003-2004. Retrieved July 4, 2004, from http://europa.eu.int/information_society/programmes/iap/docs/pdf/programmes/workprgm/work_programme_2003_04_en.pdf

European Commission (2003c). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors. COM(2003) 653 final. Brussels. Retrieved March 24, 2005, from http://europa.eu.int/eur-lex/en/com/cnc/2003/com2003_0653en01.pdf

European Commission (2004a). Commission staff working paper: Ex ante evaluation Safer Internet plus (2005-2008). COM (2004)91 final. Retrieved March 24, 2005, from http://europa.eu.int/information_society/activities/sip/docs/pdf/si_plus/exante.pdf

European Commission (2004b). *Eurobarometer: Illegal and harmful content on the Internet*. Retrieved April 12, 2005, from http://europa.eu.int/information_society/activities/sip/docs/pdf/reports/eurobarometer_survey.pdf

European Commission (2004c). Proposal for a decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies. COM(2004) 91 final. Brussels. Retrieved March 24, 2005, from http://www.europa.eu.int/information_society/activities/sip/docs/pdf/si_plus/acte_en.pdf

European Commission Working Party (1996). Report on illegal and harmful content on the Internet. Retrieved March 11, 2005, from http://europa.eu.int/ISPO/legal/en/internet/wpen.html

European Commission Working Party (1997, June 4). Interim report on initiatives in EU member states with respect to combating illegal and harmful content on the Internet. Vol. 7. Retrieved March 11, 2005, from http://europa.eu.int/ISPO/legal/en/internet/wp2en-chap.html

European Parliament (1997). Resolution on the Commission Communication on Illegal and Harmful Content on the Internet (COM(96)0487 C4-0592/96). PE 259.181, 29-35. *The Official Journal of the European Communities, C150*, 38.

EXZONE (2001a, July 30). IVANCITY JEOPSOK BULNEUNGGWA GONGDONGPAEOP [IVANCITY access denied and cooperative strike]. Retrieved April 5, 2005, from http://outpridekorea.com/ttboard/ttboard.cgi?act=view&code=21&bname=NOTICE&page=1

EXZONE (2001b, October 31). EXZONE SAYONGBANGBEOP ANNAE [EXZONE use guide]. Retrieved April 5, 2005, from Archived EXZONE Website: http://exzone.com/html/t.html

EXZONE (2001c, November 9). EXZONE PAEOPE DEULEOGAMYEO [EXZONE goes on a strike]. Retrieved November 15, 2001, from http://exzone.com

EXZONE (2004, January 1). 12WOL 13IL: DAEBEOPWON SANGGO GYEOLJEONG [31st December: An appeal to the Supreme Court] Retrieved April 5, 2005, from archived LGAAD Korea Website: http://outpridekorea.com/ttboard/ttboard.cgi?category=&search_method=&search_mode=&search_word=&act=view&code=184&bname=NOTICE&page=1&SearchBlock=1

Flint, David (2000, October 25). Streaming and regulation. In Streaming Media World Conference, Sydney. Retrieved April 18, 2005 from http://www.aba.gov.au/abanews/speeches/bcasting_info/pdfrtf/df_streamingmedia_2000.rtf

Foucault, Michel (1977). *Discipline and punish: The birth of the prison* (Sheridan, Alan, Trans.). London: Penguin Books. (Original work published 1975)

Frydman, Benoit & Rovire, Isabelle (2002, September 23). Racism, xenophobia and incitement online:European law and policy. Programme in Comparative Media Law and Policy, Oxford University. Retrieved March 18, 2005, from http://selfregulation.info/iapcoda/rxio-background-020923.htm

Fulford, Benjamin (2003). Korea's weird wired world. *Forbes.com*. Retrieved January 30, 2004, from http://www.forbes.com/forbes/2003/0721/092.html

Gibbons, Thomas (1995). Computer generated pornography. *International Yearbook of Law, Computers and Technology 9*.

GILC (1997). GILC submission on PICS. Retrieved June 7, 2002, from http://www.gilc.org/speech/ratings/gilc-pics-submission.html

GILC (1998). Regardless of frontiers: Protecting the human rights to freedom of expression on the global Internet. Retrieved January 26, 2002, from http://www.gilc.org/speech/report/

GILC (1999, September). Global Internet Liberty Campaign member statement submitted to the Internet Content Summit. Munich, Germany. Retrieved March 28, 2005, from http://www.gilc.org/speech/ratings/gilc-munich.html

Greenfield, Paul, McCrea, Philip & Ran, Shuping (1999). Access prevention techniques for Internet content filtering. Retrieved January 14, 2002, from CSIRO Website: http://www.cmis.csiro.au/Reports/filtering.pdf

Gromov, Gregory R. (1995). The roads and crossroads of Internet history. Retrieved June 23, 2004, from http://www.netvalley.com/intval1.html

Grossman, Wendy M. (1997). *Net.wars*. New York: New York University Press.

Gunningham, Neil & Rees, Joseph (1997). Industry self-regulation: An institutional perspective. *Law and Policy Vol. 19(4)*, 370-380.

Gurak, J. Laura (2001). *Cyberliteracy: Navigating the Internet with awareness*. New Haven, Connecticut and London: Yale University Press.

Habermas, Jürgen & Seidman, Steven (1989). *Jürgen Habermas on society and politics: A reader*. Boston: Beacon.

Hamilton, Stuart (2002). An overview of global Internet access barriers. In *Libraries, Conflicts and the Internet: IFLA/FAIFE Summary Report 2002* (pp. 15-30). Copenhagen, Denmark: IFLA/FAIFE.

Han, Jong-Woo (2003). Internet, social capital and democracy in the information age: Korea's defeat movement, the red devils, candle light anti-U.S. demonstration, and presidential election during 2000-2002. Systems Assurance Institute, Syracuse University. Retrieved April 29, 2005, from http://sai.syr.edu/facultypapers/Han%207-29-03.pdf

Han, Jun-Sang (1996). *SIN GYOYUK SAHOEHAK* [*New educational sociology*]. Seoul: HAK-JI SA.

Han, Wy-Soo (2003). YEONGHWA DEUNGGEUPJEWA PYOHYEONUI JAYU: TEUKHI JEHAN SANGYEONGGA DEUNGGEUPGWA GWANRYEONHAYEO [Movie Rating and Freedom of Speech -Focused on Restricted Screening Ratings]. *SEGYE HEONBEOP YEONGU, 8*, 71-111.

Hardy, Henry (1993). Hardy: The history of the Net. Retrieved June 23, 2004, from http://www.vrx.net/usenet/history/hardy/

Hauben, Ronda (1993). The development of the international computer network: From Arpanet to Usenet news. Retrieved June 22, 2004, from http://www.etext.org/Politics/Essays/arpanet

Haywood, Trevor (1998). Global networks and the myth of equality: Trickle down or trickle away? In Loader, Brian D. (Ed.). *Cyberspace divide: Equality, agency and policy in the information society* (pp. 19-34). London: Routledge.

Heins, Marjorie (2001). *Not in front of the children: "indecency," censorship, and the innocence of youth*. New York: Hill and Wang.

Heins, Marjorie & Cho, Christina (2001). Internet filters: A public policy report. National Coalition Against Censorship. Retrieved March 25, 2005, from http://www.ncac.org/issues/internetfilters.html

Hoffman, Donna L. & Novak, Thomas P. (1995). A detailed analysis of the conceptual, logical, and methodological flaws in the article: "Marketing pornography on the information superhighway." Retrieved March 11, 2001, from http://ecommerce.vanderbilt.edu/novak/rimm.review.html

Hong, Sung-Ook (2002). *PANOPTICON: JEONGBO SAHOE JEONGBO GAMOK* [*Panopticon: Information society, information prison*]. Seoul: CHAEKSESANG.

Hong, Sung-Tae (2001, June 26). INTERNET NAEYONG DEUNGGEUPJEUI MUNJEJEOM [A issue of the Internet content rating system]. In JEONGBO TONGSIN GEMYEOL BANDAE GONGDONG HAENGDONG [United Action Group Against Information and Communication Censorship], Conference report: *JEONGBUWI INTERNET NAEYONG GYUJEWA PYOHEONUI JAYU, MUEOSI MUNJEINGA?* [*Governmental Internet content rating system and freedom of expression, what is the issue?*] (pp. 16-22). Retrieved April 2, 2005, from http://freeonline.or.kr/maybbs/pds/free/allim/free0626.hwp

Hong, Sung-Tae (2003, December). DASI INOSCHOOLEUL SANGGAKHANDA (Rethinking of iNOSCHOOL). Retrieved July 7, 2004, from Cultural Action Website: http://culturalaction.org/maynews/readview.php?table=ca_issue&item=&no=166

House of Commons, Culture, Media and Sport Committee (2001, March). Second Report. Session 1999-2000. Retrieved March 23, 2005, from http://www.parliament.the-stationery-office.co.uk/pa/cm200001/cmselect/cmcumeds/161/16102.htm

House of Commons, Home Affairs Committee (1994, February 9). First report: Computer pornography: Report, together with the proceedings of the committee, minutes of evidence and appendices. London: HMSO.

House of Lords, Select Committee on Science and Technology (1996, July 23). Fifth Report: Information society: Agenda for action in the UK. London: HMSO. Retrieved March 12, 2005, from http://www.parliament.the-stationery-office.co.uk/pa/ld199596/ldselect/inforsoc/inforsoc.htm.

Hudson, David (1998). Clinton signs CDA 2 into law; cyber-liberty group respond with lawsuit. Retrieved May 2, 2003, from Freedom Forum Website: http://www.freedomforum.org/speech/1998/10/22cda.asp

Human Rights Watch (2001, July). Freedom of expression and the Internet in China: A Human Rights Watch backgrounder. Retrieved March 7, 2005, from the Human Rights Watch Website: http://www.hrw.org/backgrounder/asia/china-bck-0701.pdf

Hwang, Sang-Jae (1996). MINJUJEOK COMMUNICATION GONGGANEURO CYBERSPACEUI GANEUNGSEONGGWA HANGYE [A Feasibility and limitation of cyberspace as a sphere for democratic communication]. *HANGUK EONRON HAKBO, 38*, 43-86.

Hwang, Seung-Heum & Hwang, Sung-Gi (2003). *INTERNETEUN JAYUGONGGANINGA?* [*Is the Internet a space of freedom?*]. Seoul: Communication Books.

Hwang, Seung-Heum, Hwang, Sung-Gi, Kim, Gi-Yeon & Choi, Seung-Hun (2004). *INTERNET JAYUL GYUJE* [*Internet self-regulation*]. Seoul: Communication Books.

Hwang, Sung-Gi (2000, November). CYBERSPACEWA BULON TONGSIN GYUJE [Cyberspace and regulation of improper communications]. *HEONBEOP YEONGU. 6(3),* 153-207.

Hwang, Sung-Gi (2003, January). BULON TONGSIN GYUJEWA PYOHYEONUI JAYU [Improper communication regulation and freedom of expression]. *INTERNET BEOPRYUL, 15*, 106-138.

ICANNWatch (2003). ICANNWatch FAQ. Retrieved January 23, 2004, from http://www.icannwatch.org/faq.shtml

ICEC (1999, December). *INTERNET NAEYONG DEUNGGEUPJEUI GUKNAE DOIP BANGANE KWANHAN YEONGU* [*A technical review of the Internet content rating system in Korea*]. Seoul: ICEC.

ICEC (2003). Activities: Information Communications Ethics Committee. Retrieved April 1, 2005, from http://www.icec.or.kr/

ICEC & NCA (1999, December). *SEVERYONG YUHAE JEONGBO CHADAN DOGU GAEBAL* [*The development on the illegal and harmful content blocking tools for server systems*] Seoul: MIC.

ICRA (1999). Internet Content Rating Association formed to provide global system for protecting children and free speech on the Internet. Retrieved March 10, 2001, from http://www.icra.org/press/p1.htm

ICAR (2002). Internet industry leaders gather for launch of ICRAfilter. Retrieved October 25, 2004, from http://www.icra.org/press/icrafilter/

ICRA (2003a). Customisation and personalisation through RDF. Retrieved June 6, 2003, from http://www.icra.org/_en/press/#rdf

ICRA (2003b). European project empowers Internet users with the release of ICRAplus. Retrieved January 29, 2003, from http://www.icra.org/press/icraplus/

IDOO (2002a). GAJEONGGIPE FORKCRANE DEULIDAKCHINNAL [The day a family house was attacked]. Retrieved July 6, 2004, from http://www.idoo.net/?menu=outschool&sub=outschool3&no=4&mode=read

IDOO (2002b). HEOMUMAENGRANGHAN PYESWAEJOCHI, MALDO ANDOENEUN PYESWAE SAYU [Unreliable measure of closing down, unsound reason for closing down]. Retrieved July 6, 2004, from http://www.idoo.net/?menu=outschool&sub=outschool3&no=5&mode=read

IDOO (2002c). JEONGTONGYUNRIWIUI iNOSCHOOL PYESWAE IUI JEGI GEOBU [ICEC rejected iNOSCHOOL's appeal]. Retrieved July 6, 2004, from http://www.idoo.net/?menu=outschool&sub=outschool3&no=8&mode=read

IGLHRC (2001, August 23). Bigotry and censorship masquerade as protection of youth: Protest blockage of gay Internet sites. Retrieved August 4, 2002, from http://www.iglhrc.org/world/ne_asia/Korea2001Aug.html

ILPF (1998). Observation on the state of self-regulation of the Internet. Retrieved May 9, 2001, from http://ilpf.org/selfreg/whitepaper.htm

IMF (2000, August 23). IMF completes final review of Korea program. Washington DC. Retrieved May 26, 2002, from http://www.imf.org/external/np/sec/nb/2000/nb0072.htm

IMF (2001, August 22). IMF Managing Director Congratulates Korea on Early Repayment of 1997 Stand-By Credit. IMF News Brief No. 01/82. Retrieved April 19 2005, from http://www.imf.org/external/np/sec/nb/2001/nb0182.htm

Industry Standard (2001). Libraries spearhead attack on cyber-porn law. *Reuters*. Retrieved September 11, 2001, from http://www.thestandard.com/article/0,1902,22977,00.html

INHOPE (2002). First report. Retrieved March 25, 2005, from http://www.inhope.org/doc/report2002.pdf

INHOPE (2003, June 5). INHOPE white paper on the work of the Internet hotline network. Retrieved March 14, 2004, from http://www.inhope.org/doc/2003-0606-white-paper.pdf

INHOPE (2004a). History of INHOPE. Retrieved June 11, 2004, from http://www.inhope.org/en/about/history.html

INHOPE (2004b). Mission and objectives statement. Retrieved June 12, 2004, from http://www.inhope.org/doc/mission.pdf

International Centre for Human Rights and Democratic Development (2001). Review of China's Internet regulations and domestic legislation. Retrieved March 11, 2004, from http://www.ichrdd.ca/english/commdoc/publications/globalization/legislationInternetChinaEng.pdf

Internet Association of Korea (2005, March). A brief history of the Internet in Korea. Retrieved March 30, 2005, from http://www.internethistory.or.kr/breifhistory/Internet-Brief-History(3.28).doc

Internet Free Expression Alliance (1998, July 14). Joint letter to the United States Senate. Retrieved January 25, 2004, from http://www.ifea.net/joint_ltr_7_14.html

Internet Industry Association (1999). Internet Industry codes of practice: Codes for industry self regulation in areas of Internet content pursuant to the requirements of the Broadcasting Services Act 1992 as amended. Australia. Retrieved June 16, 2004, from http://www.iia.net.au/code6.html

INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE [United Counter-plan Commission against Government Internet Censorship] (2002a, May 31). JEONGBOTONGSINYUNRIWINEUN GUNDAEBANDAEWONDONG HOMEPAGEE DAEHAN "IYONG JEONGJI 2GAEWWOL"UI SIJEONGYOGUREUL JEUGAK CHEOLHOEHARA [ICEC should immediately withdraw the "2 months suspension" order on the anti-army hompage]. In INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE (2003, February), *2002 GEOMYEOL BAEKSEO* [*2002 Censorship Whitepaper*]. Retrieved April 1, 2005, from http://cham2.jinbo.net/maybbs/pds/nocensor/pds/white2002.hwp

INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE [United Counter-plan Commission against Government Internet Censorship] (2002b, October 11). JEONGI TONGSIN SAEOP BEOP JE53JO WIHEON GYEOLJEONGGWA JEONGBO TONGSINBUUI GAEJEONGANE DAEHAN SIMINDANCHE UIGYEON [Civil orgainsation's opinion on the unconstitutional decision of the Telecommunications Business Act and the MIC's reformed bill]. Retrieved April 8, 2005, from http://freeonline.or.kr/maybbs/pds/free/allim/irat2002.hwp

INTERNET GUKGA GEOMYEOL BANDAEREUL WIHAN GONGDONG DAECHAEK WIWONHOE [United Counter-plan Commission against Government Internet Censorship] (2003, February). *2002 GEOMYEOL BAEKSEO* [*2002 Censorship Whitepaper*]. Retrieved April 1, 2005, from http://cham2.jinbo.net/maybbs/pds/nocensor/pds/white2002.hwp

Internet Self-Regulation Forum (2002a, July). BULON TONGSIN GYUJE SYSTEME DAEHAN HEONBEOP JAEPANSOUI WIHEON GYEOLJEONGEUL HWANYEONGHAMYEO [Welcome the Constitutional Court's decision on the improper communication regulation system]. Retrieved March 21, 2004, from http://www.r3net.org

Internet Self-Regulation Forum (2002b, October). INTERNET NAEYONG GYUJEUI JINJEONGHAN CHULBALSEONE SEOGI WIHAE [For the new start of the Internet content regulation policy]. Retrieved December 15, 2002, from http://www.r3net.org

Internet Self-Regulation Forum (2003, February). ANJEONHAN INTERNETEUL GUHYEONHAGI UIHAN JEONGCHAEK JEAN [The policy proposal for safer Internet]. Retrieved March 21, 2004, from http://www.r3net.org

INTERNETSI IRWONAEN SEONGEO HYEOKMYEONGUI MYEONGAM [Light and darkness of the Internet election revolution] (2002, December 22). *The Hankyoreh Newspaper*. Retrieved July 6, 2004, from http://www.hani.co.kr/section-001001000/2002/12/001001000200212222015952.html

Irving, Larry (1997). Introduction from the Assistant Secretary, National Telecommunications and Information Administration. In US Department of Commerce (Ed.), Privacy and self-regulation in the information age. Washington DC. Retrieved March 12, 2004, from http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

ISPA UK, LINX & the Safe-Net Foundation (1996, September 23). R3 safety-net: Rating reporting responsibility for child pornography & illegal material on the Internet: An industry proposal. Retrieved June 11, 2001, from the IWF Website: http://www.iwf.org/about/r3_safety.html

ITU (2003, September). *ITU Internet Reports: Birth of Broadband.* Geneva, Switzerland.

IWF (1999). The Internet Watch Foundation second annual report. Retrieved June 16, 2004, from http://www.iwf.org.uk/about/annual_report/annual98.html

IWF (2001). The Internet Watch Foundation annual report 2000. Retrieved December 27, 2001, from http://www.iwf.org.uk/about/annual_report/annual2000.rtf

IWF (2002). The Internet Watch Foundation annual review 2001. Retrieved May 7, 2003, from http://www.iwf.org.uk/about/annual_report/ar2002.htm

IWF (2003a). The Internet Watch Foundation annual review 2002. Retrieved May 7, 2003, from http://www.iwf.org.uk/about/annual_report/annual2002.htm

IWF (2003b). Safe surfing: Software tools. Retrieved June 2, 2003, from http://www.iwf.org.uk/safe_surfing/software_tools.html

Jang, Dong-Jin (2003). Distributive justice in Korean politics after the IMF bailout. *Global Economic Review, 31(4)*, 57-73.

Jang, Yo-Kyong (2001, February). TONSIN JILSEO HWAKRIP BEOP, MUEOSI MUNJEYEOSEUMYEO EODDEON MUNJEGA NAMANEUNGA? [Communication Order Establishment Law, What was the issue?]. In JEONGBO TONGSIN GEOMYEOL BANDAE GONGDONG HAENGDONG [United Action Group Against Information and Communication Censorship], 2000NYEON TONGSIN JILSEO HAWKRIP BEOP BANDAE BAEKSEO [2000 white paper: Fight against the Communication Order Establishment Law] (pp. 2-10). Retrieved April 2, 2005, from http://free.jinbo.net/doc/action2000.hwp

Jang, Yo-Kyong (2002, January 24). DONGSEONGAEJAUI INTERNETDEUNGGEUPJE SSAUM [A Gay's fight against the Internet content rating system]. *THE HANKYOREH SHINMUN*. Retrieved July 7, 2004, from http://www.hani.co.kr/section-005100025/2002/01/005100025200201242056100.html

Jenkins, Philip (2001). *Beyond tolerance*. New York: New York University Press.

Jeon, Tae-Guk (2002, December). HANGUKUI JABONJUUI BALJEONGWA YUGYOUI YEOKHWAL [On the Role of Confucianism in the Capitalistic Development of Korea]. 2002NYEONDO HANGUKSAHOEHAKHEO HUGISAHOEHAKDAEHOE [2002 Korean Sociological Association, The Second Sociology Conference]. Retrieved March 29, 2005, from http://tkjeon.kangwon.ac.kr/pro_pds/한국의%20 발전과%20 유교의%20 역할(021203).doc

Jeon, Tae-Guk (2003). MAX WEBERUI YUGYO THESEWA HANGUK SAHOE [Max Weber's Confucian these and Korean society]. *SAHOEWA IRON, 2*, 39-84.

Jeong, Jae-Suk (2001, May 28). GEOMCHALUI JAUIJEOK EUMRANMUL JATTAE [Arbitrary obscenity standard of the proscesutor]. *THE HANKYOREH SHINMUN*. Retrieved April 1, 2005, from http://www.hani.co.kr/section-001033000/2001/05/p001033000200105281820055.html

Jeong, Wan (2001). BULGEONJEONSITEUI BUMRAMGWA BEOPJEOKGYUJE [Flooding of unhealthy site and legal regulation]. *HYEONGSA JEONGCHAEK YEONGU SOSIK, 9/10*.

JEONGBO TONGSIN GEOMYEOL BANDAE GONGDONG HAENGDONG [United Action Group Against Information and Communication Censorship] (2001, February). *2000NYEON TONGSIN JILSEO HAWKRIP BEOP BANDAE BAEKSEO* [*2000 white paper: Fight against the Communication Order Establishment Law*]. Retrieved April 2, 2005, from http://free.jinbo.net/doc/action2000.hwp

JEONGBO TONGSIN YUNRIWI, DUDALJJAE GINEUNG MABI [ICEC, hamstring for two month] (2002, September 1). *YEONHAP News*. Retrieved April 9, 2005, from http://news.naver.com/news/read.php?mode=LOD&office_id=001&article_id=0000230508

JEONGBO TONGSINBUUI TONGSIN JILSEO HWAKRIPBEOP IPBEOP YEOGOE DAEHAN SIMIN SAHOE DANCHEUI IPJANG ["Civil social organisations' standpoint concerning a preliminary notice of the Communication Order Establishment Law"] (2000, September 20). *JEONGBO INKWON UNDONG NEWS* [*Information Human Rights Movement News*]. Retrieved April 1, 2005, from http://www.action.or.kr/?doc=bbs/gnuboard.php&bo_table=info_news&page=11&wr_id=399

JEONGBO TONGSINUI NAL 50DOL: Game [50th anniversary of info-communication day: Game] (2005, April 21). *SEOUL GYEONGJE*. Retrieved April 27, 2005 from http://economy.hankooki.com/lpage/special/200504/e2005042115185748640.htm

Jiang renews warning against "pernicious" Internet (2001, July 12). LatelineNews. Retrieved May 3, 2003, from http://news.1chinastar.com/news.shtml?l=english&a=express&p=1082398

Jin, Mi-Suk (2003). HAKBULGWA SAMUI BANGSIK: HAKBUL SAHOEUI BOGOSEO [HAKBUL and way of life: Report on our HAKBUL culture]. *HANGUK GYOYUK YEONGU, 9(1)*. 70-92.

JINBO Network Centre (2002a, June 28). JEONGI TONGSIN SAEOP BEOP JE53JO BULON TONGSIN JOHANGE DAEHAN WIHEON PANGYEOLEUL HWANYEONGHANDA [Welcome the Constitutional Court's decision on Clause 53 of the Telecommunication Business Act]. Retrieved March 21, 2004, from http://cham2.jinbo.net/maybbs/view.php?db=nocensor&code=news&n=11&page=2

JINBO Network Centre (2002b, August 2). JEONGBO TONGSINBUNEUN HEONBEOP JAEPANSO WIHEON GYEOLJEONGEUL WAEGOKMALRA [Do not strain the Constitutional Court's decision]. Retrieved March 21, 2004, from http://cham2.jinbo.net/maybbs/view.php?db=nocensor&code=news&n=16&page=2

Johnson, David & Post, G David. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review, 48(1367).* Retrieved July 6, 2004, from http://www.cli.org/X0025_LBFIN.html

Johnson, M. Glen (1998). A Magna Carta for mankind: Writing the Universal Declaration of Human Rights. In Johnson, M. Glen & Symonides, Janusz (Eds.), *The Universal Declaration of Human Rights: A history of its creation and implementation 1948-1998* (pp. 19-75). Paris: UNESCO Publishing.

Jung-Chun (1999, August 1). MISEONGNYEONJA CHULIPGYUJE TORONHU: IPJANGJEONGRI [After the discussion on the issue of people under 18 years of age and their access to EXZONE]. Retrieved October 8, 2002, from http://exzone.com/xxxzzz

Kahn, Jennifer (2002). It's alive: From airport tarmacs to online job banks to medical labs, artificial intelligence is everywhere. *Wired, Vol. 10.03,* 74-77.

Kaiser Family Foundation (2002). See no evil: How Internet filters affect the search for online health information: Executive summary. Retrieved 25 March 2005, from http://www.kaisernetwork.org/health_cast/uploaded_files/Internet_Filtering_exec_summ.pdf

Kang, Hyeon-seok (1998). IYONGJAGA JUINDOENEUN JINBOJEOK JEONGBOINFRA [Progressive information infrastructure for users]. *SAHOE PYEONGRON GIL, 98(7),* 223.

Kang, Yeen-Kyu (2005, March 16). CHOGOSOK INTERNET SIJANG DONGHYANG [Trend of the broadband Internet market]. *JEONGBO TONGSIN JEONGCHAEK 17(5).* 28-32.

KCPB (2000). INTERNET IYONG CHOKJINEUL WIHAN PC BANG GAESEONGAEHOEK [The PC-bang improvement plan for promoting Internet usage]. Seoul, South Korea. Retrieved May 23, 2002, from http://www.cpb.or.kr/

Keller, Daphne & Verhulst, Stefaan (2000). Parental control in a converged communications environment self-regulation, technical devices and meta-information: Final report for the DVB Regulatory Group. Oxford: University of Oxford, Progamme in Comparative Media Law and Policy. Retrieved June 5, 2003, from http://europa.eu.int/comm/avpolicy/regul/new_srv/dvbgroup.pdf

Kerr, David (2000). Internet Content Rating for Europe, Final Report. Retrieved March 27, 2005, from http://europa.eu.int/ISPO/iap/INCOREexec.html

KESA (2001, May 29). The game industry in 2000. Retrieved July 17, 2001, from http://www.game.or.kr/common/press/press_view.asp?idx=94

Kim, Chan-Jin (2000, December). Korean attitudes towards law. *Pacific Rim Law & Policy Journal, 10*, 1-46.

Kim, Cheol-Wan, Jeong, Jun-Hyeon, Lee, Sang-Won & Oh, Yeong-seok (2001, December). *JEONGCHAEK YEONGU 01-05: GAEIN JEONGBO BOHO JEDO SIHAENGUI GYEONGJE SAHOEJEOK PAGEUP HYOGWA BUNSEOK YEONGU* [*Policy study 01-05: A analysis study of the economic and social ripple effect of the enforcement of personal information protection system*]. Seoul: JEONGBO TONGSIN JEONGCHAEK YEONGUWON.

Kim, Deok-hyun (2002, March 13). Korea leads OECD peers in broadband Internet service. *The Korea Times*. Retrieved July 6, 2004, from http://times.hankooki.com/times.htm

Kim, Hee-Seob (2002, November 6). Internet users pass 10 million mark. *THE CHOSUN ILBO*. Retrieved July 6, 2004, from http://english.chosun.com/w21data/html/news/200211/200211060024.html

Kim, Hyeong-Gi (1999, June 11). LEWINSKYWA OH HYEON KYEONG [Lewinsky and Oh Hyeon Kyeong]. *CHOSUN ILBO*. Retrieved March 29, 2005, from http://db1.chosun.com/cgi-bin/gisa/artFullText.cgi?where=PD=19990611&ID=9906110705

Kim, Hyeong-Jun (2003). MEDIAWA INTERNET SEONGEO WUNDONGE DAEHAN PYONGGA [Aanlysis of media and Internet election campaigns]. *2003NEUN HANGUK JEONGCHI HAKHOE CHUNGE HANKSUL HOEUI*. 94-114.

Kim, Jae-Seop (2001, June 11). JATOESAENG SITE PYESWAE NONRAN [Controversy over the site of a voluntary dropout student]. *THE HANKYOREH SHINMUN*. Retrieved April 6, 2005, from http://www.hani.co.kr/section-010100001/2001/06/010100001200106112235011.html

Kim, Ji-Ho (2002, December 16). Memorial rallies for dead girls draw crowds. *The Korea Herald*. Retrieved July 6, 2004, from http://www.koreaherald.co.kr/archives/result_contents.asp?id=200212160095&query=candle#

Kim, Jin-Hyuk (2001, Jun 28). iNOSCHOOL PYESWAE BUDANGSEONGGWA JEONGBO TONGSIN YUNRI WIWONHOEUI JALMOSE GANHAYEO (About an unfair closedown of iNOSCHOOL and the ICEC's fault). *DAEJABO, No. 61*. Retrieved July 7, 2004, from http://www.jabo.co.kr/61th/61_disc2.htm

Kim, Jin-Kyeong (1997, January). HAKGYO GYOYUK, JONJAE JACHEUI WIGI GEURIGO DAEWAN (1) [School education, a crisis of existence and an alternative]. *HANGUK GYOYUK YEONGU SOSIK, 30*, 16-24.

Kim, Jong-Seo (2003). INTERNETSANGUI EUMRANMUL GYUJE GIJUN BIGYO YEONGU: BIPANJEOK GWANJEOM [The Standard for the Regulation of the Cyber Obscenity: A Critical & Comparative Perspective]. *MINJU BEOPHAK, 24*, 207-246.

Kim, Ju-Hyun & Lee, Sang-Ju (2001, June 17). JEONGBOTONGSINYUNRIWI SIMUI JADAEGA EOPDA [The ICEC's deliberation lacks consistency]. *KYOUNG-HYANG SHINMUN*. Retrieved July 7, 2004, from http://www.khan.co.kr/news/2001/06/17/200106171924071.html

Kim, Ki-Joong (2001, October, 31). INTERNET DEUNGGEUPJEWA CHEONGSONYEON [Internet rating system and youth]. *THE HANKYOREH SHINMUN*. Retrieved April 2, 2005, from http://www.hani.co.kr/section-001055000/2001/10/001055000200110312350002.html

Kim, Ki-Joong (2003, April 3). Internet filtering, blocking and government censorship in South Korea. In 13th Annual Conference on Computers, Freedom & Privacy. Retrieved March 30, 2005, from http://socialrights.org/spip/IMG/rtf/wsis_kijoongv_eff_e.rtf

Kim, Yi-Gi (2002). *CHOESIN INTERNET BANGSONGUI IHAE* [*Understanding of the latest Internet Broadcasting*] (e-book ed.). Seoul: Communication Books.

Kiri Kiri (2004). HANGUK LESBIAN INGWON WUNDONG 10NYEONSA [Korea lesbian rights movement 10years]. *JINBO PYEONGRON, 20*. Retrieved May 1, 2005, from http://jbreview.jinbo.net/maynews/readview.php?table=organ&item=4&no=443

Korea National Statistical Office (2000). Housing by type of living quarter: by number of household. Retrieved May 31, 2002, from http://www.nso.go.kr

Krattenmaker, Thomas G. & Powe, Lucas A. Jr. (1994). *Regulating broadcast programming*. Washington DC: The AEI Press.

KRNIC (2003). 2003NYEON 4WOL INTERNET TONGGYE WOLBO [April 2003: The monthly Internet statistics]. Retrieved July 7, 2004, from http://isis.nic.or.kr/report_DD_View/upload/rep200304.pdf

Kranzberg, Melvin (1985) The information age: Evolution or revolution? In Guile, Bruce R. (Ed.), Information technologies and social transformation. Washington DC: National Academy of Engineering.

Krug, Judith, Matthews, Richard & Robinson, Cynthia (1998). Virginia residents challenge library filtering policy. Retrieved December 15, 2001, from ALA Website: http://www.ala.org/alaorg/oif/actionnews_acti0198.html

Kwon, Bok-Gi (2000, August 28). NETIZENEUN JIGEUM DEMOJUNG [Netizen is now demonstrating]. *THE HANKYOREH SHINMUN*. Retrieved April 1, 2005, from http://www.hani.co.kr/section-005002003/2000/00500200320000828190 8003.html

Lawrence, Steve & Giles, Lee (1999). Accessibility of information on the web. *Nature, 400*, 107–109.

Lee, Dong-Yeong (2002, June 14). MIGUN CHAE CHIYEO YEOJUNGSAENG DUL SAMANG [Two middle school girls were killed by a US Army vehicle]. *Donga Ilbo*, A31.

Lee, Gi-Jin (2001a, June 13). 'NUDE GYOSA,' JAECHEONGGUYEONGJANGDO GIGAK ['Nude teacher,' the reclaimed warrant is rejected]. *DONGA ILBO*, A29.

Lee, Gi-Jin (2001b, June 23). "PYOHYEONUI JAYU CHIMHAE," MUNHWAGYE BANBAL HWAKSAN ["Violation of freedom of expression," cultural organisations' protest spreads]. *DONGA ILBO,* A25.

Lee, Guk-Myeong (2001, June 12). 'JATOE SITE' PYESWAEE NETIZEN HANGUI [Netizens protest against closing down of 'a leaving school site']. *DONGA.COM.* Retrieved April 6, 2005, from http://www.donga.com/fbin/moeum?n=dstory$k_148&a=v&l=0&id=200106120031

Lee, Hae-Wan (2002, October). BULON TONGSIN GYUJEWA PYOHYEONUI JAYU [Improper communication regulation and freedom of expression]. *EONRUNGWA BEOP, 1.*

Lee, Hyo-Seong & Kim, In-Yeong (2003). TELEVISION, SHINMUN, INTERNET IYONGUI YUGWONJAUI JEONGCHI JISIK, 16DAE DAESEON GWANSIM, JEONGCHI HWALDONGE MICHINEUN YEONGHYANG BUNSEOK [Exploring the Influences of Television, Newspapers, and the Internet to Voters` Political Participation (Political Knowledge, Interest to the 16th Presidential Election, and Political Activities Participation)]. *COMMUNICATIONHAK YEONGU, 11(2).* 29-63.

Lee, Jang-Yeong & Kang, Hyo-Min (2001). JEONJA JEONGBO GONGGANESEO GUKGA DAEPYO CHUKGU TEAM SUPPORTER "BULGEUN AKMA"UI GONGDONGCHE HYEONGSEONG [Shaping the community of the national football team supporter "Red Devil" on electronic information space]. *JEONGBOWA SAHOE, 3,* 124-139.

Lee, Min-Yeong (2004). CHEONGSONYEON YUHAEMAECHEMUL GYUJE: EXZONESAGEON PANGYEOLE DAEHAN PYEONGGAWA BUNSEOK [Regulating harmful-to-youth medium material: An evaluation and analysis on the EXZONE case]. *JEONGBO TONGSIN JEONGCHAEK, 16(2),* 20-42.

Lee, Sang-Hee (2001). JEONGBO TONGSIN YUNRI WIWONHOEUI INTERNET GEOMYEOL MIT BEOPJEOK DAEEUNGE DAEHAYEO [ICEC's Internet censorship and legal counter-plan]. In JEONGBO TONGSIN GEMYEOL BANDAE GONGDONG HAENGDONG [United Action Group Against Information and Communication Censorship], *JEONGBUUI INTERNET NAEYONG GYUJEWA PYOHEONUI JAYU, MUEOSI MUNJEINGA?* [*Governmental Internet content rating system and freedom of expression, What is the issue?*] (pp. 2-15). Retrieved April 2, 2005, from http://freeonline.or.kr/maybbs/pds/free/allim/free0626.hwp

Lee, Sang-Hee (2002, January). CHEONGSONYEON YUHAE MAECHEMUL JIJEONGE DAEHAN HAENGJEONG SOSONG SOJANG [An administrative lawsuit petition concerning the harmful-to-youth material indication]. Retrieved April 5, 2005, from http://cham2.jinbo.net/maybbs/pds/nocensor/pds/엑스존행정소송.hwp

Lessig, Lawrence (1998, March). The laws of cyberspace. In the Taiwan Net '98 conference. Taipei, Taiwan. Retrieved July 7, 2004, from Harvard University, Berkman Center Website: http://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf

Lessig, Lawrence (1999). *Code and other laws of cyberspace*. New York: Basic Books.

LGAAD Korea (2001, November 27). JEONGTONGYUNE JEONGBO GONGGAE CHEONGGU-EXZONE JAESIMUIE DAEHAN [A request for opening ICEC Information concerning redeliberation on EXZONE]. Retrieved April 5, 2005, from http://outpridekorea.com/ttboard/data/NOTICE/재심의정보공개청구.hwp

LGAAD Korea (2002, January 9). BODO JARYO: 'DONGSEONGAEJA CHABYEOLBEOP CHEOLPYAE'WA 'INTERNET NAEYONGDEUNGGEUMJE PYAEJI'REUL WIHAN 'HAENGJEONGSOSONG' GIJAHOEGYEON [A Press release: The press conference of an administrative lawsuit for 'repeal of homosexuality discrimination law' and 'abolition of Internet content rating system']. Retrieved April 5, 2005, from http://outpridekorea.com/ttboard/data/NOTICE/기자회견보도자료.hwp

Lifton, Robert (1986). *The Nazi doctors: Medical killing and the psychology of genocide*. London: Macmillan.

Liikanen, Erkki (2004, April 15). Internet governance the way ahead. SIDN event. Hague. Retrieved March 16, 2005, from http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=SPEECH/04/191|0|RAPID&lg=EN

Lim, Yee Fen (2003, December). Law and regulation in cyberspace. In Sourin, Alexei (Chair), *Creating new worlds*. 2003 International Conference on Cyberworlds. Singapore.

Loader, Brian D. (1998). Cyberspace divide: Equality, agency and policy in the information society. In Loader, Brian D. (Ed.). *Cyberspace divide: Equality, agency and policy in the information society* (pp. 3-16). London: Routledge.

Machill, Marcel (2001). Who controls the Internet? The Bertelsmann Foundation's recommendations for Internet governance. Berlin: The Bertelsmann Foundation. Retrieved March 23, 2005, from http://www.democratic-internet.de/berlin2001/recommendations.pdf

Machill, Marcel, Hart, Thomas & Kaltenhäuser, Bettina (2002). Structural development of Internet self-regulation. *Info-The journal of policy, regulation and strategies for telecommunications, 4(5)*, 39-55.

Macintyre, Donald (2000, December 11). Wired for life. *TIME Asia, 156(23).* Retrieved April 20, 2005, from http://www.time.com/time/asia/magazine/2000/1211/cover1.html

Malone, Steve (2004, August 12). Britain goes digital media crazy. *Computer Byuer*. Retrieved 15 September, 2004, from http://www.pcpro.co.uk/?http://www.pcpro.co.uk/news/news_story.php?id=61749

Manchester, Colin (1996). More about computer pornography. *Crime Law Review*. 645-649.

McGauran, Peter (2000, January 6). Managing access to Internet content. Australia: Department of Communications, Information Technology and the Arts. Retrieved July 7, 2004, from http://www.dcita.gov.au/Article/0,,0_1-2_1-4_14749,00.html

Meeks, Brock (1995). Jacking in from the "point-five percent solution" port. *CyberWire Dispatch*. Retrieved June 4, 2004, from http://elab.vanderbilt.edu/research/topics/cyberporn/brock.rimm.reviewfix.htm

Mendels, Pamela (1999). Internet rating system plans to globalise. *The New York Times*. Retrieved February 6, 2002, from http://www.nytimes.com/library/tech/99/09/cyber/articles/25ratings.html

MIC (1999a, January). Korea's vision for the information society. Retrieved 29, 2002, from http://www.mic.go.kr/

MIC (1999b, March). Cyber Korea 21: An information vision for constructing a creative knowledge-based nation. Seoul, South Korea. Retrieved July 7, 2004, from the Informatization Promotion Committee Website: http://www.ipc.go.kr/intra/english.nsf/3f90799c2c43d51f492569550007981f/1637e9c71294c5aa492569700023364f/$FILE/ckfull.doc

MIC (1999c). The Internet PC accelerates a construction of knowledge-information infrastructure. Retrieved May 29, 2002, from http://www.mic.go.kr/

Mill, John Stuart (1974, Himmelfarb, Gertrude. Ed.). On liberty. London: Penguin Books. (Original work published 1859)

Miller, James (Ed.) (1996). PICS label distribution label syntax and communication protocols. Retrieved February 6, 2002, from http://www.w3.org/TR/REC-PICS-labels

Milne, Claire (2002). Regulation and the Internet. Retrieved June 18, 2004, from http://www.communicationsbill.gov.uk/responses/Antelope%20Consulting.doc

Milton, John (1951, Sabine, George H. Ed.). Areopagitica and of education. New York: Harlan Davidson. (Original work published 1644)

Min, Jae-Hong, Kim, Seong-Han & Lee Jeong-Hwa (2004, April). INTERNET NAEYONG SEONBYEOL GISUL DONGHYANG BUNSEOK [An analysis of Internet content filtering technology]. *JEONGBO TONGSIN DONGHYANG BUNSEOK*, 19(2), 117-126.

Min, Kyeong-Bae (2001, July 26). ONLINE SIWI GYEOLJEONGPAN 'SITE PAEOP' [A definitive Online demonstration 'Site strike']. *JUGAN DONGA, 294*. Retrieved April 2, 2005, from http://www.donga.com/docs/magazine/weekly_donga/news294/wd294jj020.html

Minister for Communications, Information Technology and the Arts (2000, September). Six-months report on co-regulatory scheme for Internet content regulation. Australia: Department of Communications, Information Technology and the Arts. Retrieved October 9, 2004, from http://www.dcita.gov.au/download/0,2720,4_113627,00.rtf

Minister for Communications, Information Technology and the Arts (2001, April). Six-months report on co-regulatory scheme for Internet content regulation: July to December 2000. Australia: Department of Communications, Information Technology and the Arts. Retrieved June 16, 2004, from http://www.dcita.org.au/download/0,2118,4_113733,00.doc

Minister for Communications, Information Technology and the Arts (2002, April). Six-months report on co-regulatory scheme for Internet content regulation: January to June 2001. Australia: Department of Communications, Information Technology and the Arts. Retrieved March 6, 2005, from http://www.dcita.gov.au/__data/assets/file/11560/Six-month_report_on_co-regulatory_scheme_for_internet_content_regulation_January_to_June_2001.rtf

Mitchell, William J. (1995). *City of bits: Space, place and the infobahn.* Cambridge, Massachusetts: MIT Press.

Moon, Jae-Wan (2003). Obscenity laws in a paternalistic country: The Korean experience. *Washington University Global Studies Law Review*, 2, 353-390.

Murphy, M. Paula & Blackman, Colin (1999). Communications regulation in the global information society. *International Journal of Communications Law and Policy, Issue 3.* Retrieved January 26, 2002, from http://www.digital-law.net/IJCLP/3_1999/ijclp_webdoc_11_3_1999.html

Na, Seoung-Yeop (2002a, October 29). SEONGINMUL PANJEONG 'LINEAGE' GWAGYEOKSEONG WANHWAHAE JAESIM SINCHEONG [Adult graded 'Lineage' requests redeliberation]. *DONGA ILBO*, A30.

Na, Seong-Yeop (2002b, November 15). Online game Lineage "15SE IYONGGA" PANJEONG [Online game Lineage receives the "15 years-old" grade]. *DONGA ILBO*, A29.

National Consumer Council (2000). Models of self-regulation: An overview of models in business and the professions. Retrieved March 22, 2005, from http://www.ncc.org.uk/regulation/models_self_regulation.pdf

Neumann, A. Lin (2001). The Great Firewall: In the world's fastest-growing Internet market, Chinese Communist authorities are trying hard to regulate online speech. Retrieved January 21, 2002, from Committee to Protect Journalist Website: http://www.cpj.org/Briefings/2001/China_jan01/China_jan01.html

NCA (2001). *2001 HANGUK Internet BAEKSEO [2001 Korea Internet White Paper]*. Seoul: NCA.

NCA (2002). *2002 HANGUK Internet BAEKSEO [2002 Korea Internet White Paper]*. Seoul: NCA.

NCA (2004). INTERNET NAEYONG GYUJE JEONGCHAEKUI JINDANGWA GAESON GWAJE [Evaluation of Internet content regulatory policy and the task of reform]. *NCA CIO Report, 04-14.*

Newey, Adam (1999). Freedom of expression: Censorship in private hands. In Liberty (Ed.), *Liberating cyberspace*: Civil liberties, human rights and the Internet (pp. 13-43). London: Pluto Press.

Nielsen//NetRatings (2001a). South Korea and Taiwan dominate Asian Internet usage. Retrieved May 14, 2002, from http://www.nielsen-netratings.com/pr/pr_010308.pdf

Nielsen//NetRatings (2001b). Korea claims 23 of world's 100 biggest locally accessed web properties but US still home of global properties. Retrieved May 14, 2002, from http://www.nielsen-netratings.com/pr/pr_010905_korea.pdf

Nielsen//NetRatings (2002): Nielsen//NetRatings reports a record half billion people worldwide now have home Internet access. Retrieved May 14, 2002, from http://www.nielsen-netratings.com/pr/pr_020306_eratings.pdf

Nofilters.org (2000). Frequently asked questions about filtering and censorware in public libraries. Retrieved September 1, 2001, from http://www.nofilters.org/faq/section_a.html

O'Brien, Jim (1996, January). Teach your children and save money. *Computer Shopper, 16 (1)*, 667.

OECD (1996). The knowledge-based economy (OECD/GD(96)102). Paris.

OECD (1998, October 28). Working party on telecommunication and information services policies: Internet infrastructure indicators (DSTI/ICCP/TISP(98)/Final). Paris.

OECD (2001, October 29). Working party on telecommunication and information services policies: The development of broadband access in OECD countries (DSTI/ICCP/TISP(2001)2/FINAL). Paris.

OECD (2003). *OECD Communications Outlook 2003*. Paris.

Office of the UN High Commissioner for Human Rights (2003, September 5). Core document forming part of the reports of states parties: Republic of Korea. HRI/CORE/1/Add.125. Geneva, Switzerland.

Office of the UN High Commissioner for Human Rights (2004). Status of ratifications of the principal international human rights treaties. Retrieved February 17, 2005, from http://www.unhchr.ch/pdf/report.pdf

OFLC (1999). Guidelines for the classification of publications. Sydney, Australia. Retrieved July 6, 2004, from http://www.oflc.gov.au/resource.html?resource=63&filename=63.pdf

Ogus, Anthony (1992). Regulatory law: Some lessons from the post. *Legal Studies, 12.*

Ogus, Anthony (1994). *Regulation: legal form and economic theory*. Oxford: Clarendon Press.

Ogus, Anthony. (1995). Rethinking self-regulation. *Oxford Journal of Legal Studies, 15*, 97-108.

Oh, Se-Rin (2000, October 12). GYEONGCHAL, "JEONGTONGBU HOMEPAGE MABI, NAEBU GYEOHAM DDAEMUN" [Police says, "MIC homepage crash is caused by an internal fault"]. *DONGA ILBO*. Retrived April 3, 2005, from http://www.donga.com/fbin/searchview?n=200010120264

Oh, Yoon-Ju (2001, May 27). ALMOMSAJIN HOMEPAGE GEJE GYOSA YEONGJANG [Teacher who posts a nude picture to his homepage arrested]. *THE HANKYOREH SHINMUN*. Retrieved March 31, 2005, from http://www.hani.co.kr/section-005000000/2001/05/005000000200105271955005.html

OLHAE GUKNAE GAME SIJANG 4JOWON NEOMEOSEO [Domestic gmae market's revenues exceed 4 trillion KRW] (2003, January 11). *THE HANKYOREH SHINMUN*. Retrieved April 29, 2005, from http://www.hani.co.kr/section-010100006/2003/01/p010100006200301110917109.html

ONLINE GAME BUJAKYONG SAHOEMUNJERO BUGAK [Ill effects of online games bring social issues] (2002, March 29). *THE HANYOREH SINMUN*. Retrieved July 6, 2004, from http://www.hani.co.kr/section-005000000/2002/03/005000000200203290736085.html

Online Policy Group (2001). Why Blocking Technology Can't Work. Retrieved May 29, 2003, from http://www.onlinepolicy.org/research/blockcantwork.shtml

Park, Hee-Yeong (2000). CYBEREUMRANMULE DAEHAN HYEONGBEOPJEOK DAEEUNGBANGAN: JEONGITONGSINGIBONBEOPSANG JEONGITONGSINYEOKMUIYONG EUMRANMULJOEUI HAESEOKEUL JUNGSIMEURO [Construction of criminal law for fighting cyber pomography]. *BEOPHAK YEONGU, 41(1)*, 249-286.

PCMLP (2003, March). IAPCODE report on global state of self-regulation. Retrieved March 21, 2005, from http://selfregulation.info/iapcoda/030329-selfreg-global-report.htm

PCMLP (2004, April). IAPCODE final report: Self-regulation of digital media converging on the Internet: Industry codes of conduct in sectoral analysis. Retrieved March 22, 2005, from http://selfregulation.info/iapcoda/0405-iapcode-final.pdf

Perine, Keith (2000, July 25). The trouble with regulating hatred online. *The Industry Standard.* Retrieved March 18, 2005, from http://archives.cnn.com/2000/TECH/computing/07/25/regulating.hatred.idg/

Pierlot, Paul (2000, July). Self-regulation of Internet content: A Canadian perspective. In Guedon, Jean-Claude & Murai, Jun (Co-Chairs), *Global distributed intelligence for everyone*. INET 2000 The Internet Global Summit. Yokohama, Japan. Retrieved July 6, 2004, from http://www.isoc.org/inet2000/cdproceedings/8k/8k_2.htm

Pinard, Frédéric (1998). European Commission: Action plan on promoting safe use of the Internet. IRIS Legal Observations of the European Audiovisual Observatory. Retrieved March 14, 2005, from http://merlin.obs.coe.int/iris/1998/1/article1.en.html

Photography: The pioneers (2002). *The Britannica Encylopaedia* (2002 standard ed.). Chicago: Britannica.

Pool, Ithiel de Sola (1983). *Technologies of freedom*. Cambridge, Massachusetts: The Belknap Press of Harvard university Press.

Poster, Mark (1997). Cyberdemocracy: Internet and the public sphere. In Porter, David (Ed.) *Internet culture* (pp. 201-217). New York: Routledge.

Pountain, Dick (2003). *The Penguin concise dictionary of computing*. London: Penguin Books.

Price, Monroe & Verhulst, Stefaan (2000). The concept of self-regulation. In Waltermann, Jens & Machill, Marcel (Ed.), *Protecting our children on the Internet* (pp. 133-198). Gűtersloh, Germany: Bertelsmann Foundation Publishers.

PureSight Inc. (2004, March). Dynamic filtering of Internet content: An overview of next generation filtering technology. Retrieved June 16, 2004, from http://www.icognito.com/Static/Binaries/Resource/dynamic_filtering_whitepaper_03_04_0.pdf

Ra, Do-Sam (2003, April 25). HANGUK INTERNETUI BALCHEONGWA CYBER MUNHWAUI IHAE [Development of the Internet and understanding of cyber culture in Korea]. SOGANG DAEHAKGYO SAHOE GWAHAK YEONGUSO CHUNGYE HAKSUL DAEHOE [Institute of Social Sciences SOGANG University, Spring Academic Conference]. Retrieved April 21, 2005, from http://www.sogang.ac.kr/~ssrc/social/research/030425_la.hwp

Raab, Charles D. (1997). Privacy, democracy, information. In Loader, Brian D. (Ed.). *The governance of cyberspace* (pp. 155-174). London: Routledge.

Ramadorai, S. (2000, November 27). Towards the Internet era. *The Economic Times*. Retrieved Spetember 14, 2004, from http://economictimes.indiatimes.com/articleshow/17172359.cms

Reagle, Joseph (1999). Why the Internet is good: Community governance that works well. Retrieved June 29, 2004, from Harvard University, Berkman Center Website: http://cyber.law.harvard.edu/people/reagle/regulation-19990326.htm

Resnick, Paul (1999). PICS, censorship, & intellectual freedom FAQ. Retrieved February 6, 2002, from http://www.w3.org/PICS/PICS-FAQ-980126.html

Resnick, Paul & Miller, James (1996). PICS: Internet access controls without censorship. *Communications of the ACM, 39(10)*, 87-93.

Rhee, In-Yong (2003, Spring) The Korean election shows a shift in media power. *Nieman Reports*, pp. 95-96.

Rheingold, Horward (2000). *The Virtual Community: Homesteading on the Electronic Frontier* (Rev. ed.). Cambridge, Massachusetts: MIT Press.

Rimm, Marty (1995). Marketing pornography on the information superhighway. *Georgetown Law Journal, 83(5)*, 1849-1934.

Robertson, Geoffrey & Nicol, Andrew (1992). *Media law* (3rd ed.). London: Penguin Books.

Rodriquez, Felipe (2003). Burning the village to roast the pig: Censorship of online media. In OSCE (Ed.), *From Quill to Cursor: Freedom of the Media in the Digital Era* (pp.85-109). Vienna: OSCE.

Sautede, Eric (1996). The Internet in China between the constable and the gamekeeper. *China Perspectives, 4*, 6-8.

Savada, Andrea Matles & Shaw, William (Eds.)(1992). *South Korea: A country study* (4th ed.). Federal Research Division, Library of Congress. Washington D.C.

Schmitter, P.C. (1985). Neo-corporatism and the state. In Grant, Wyn (Ed.), *The political economy of corporatism* (pp. 32-62). London: Macmillan.

Schrader, Alvin (1999, August 25). Internet filters: Library access issue in a cyberspace world. In 65th IFLA Council and General Conference. Bangkok, Thailand. Retrieved July 6, 2004, from http://www.ifla.org/faife/papers/others/schrader.pdf

Science, Technology, Information and Telecommunication Committee of the National Assembly (2000, December). JEONGBO TONGSIN CHOKJIN DEUNGE GWANHAN BEOPRYUL GAEJEONG BEOPRYULAN GEOMTOBOGOSEO [A report on the Reformed Bill of Act on Promotion of Information and Communication Network Utilisation and Information Protection, etc.]. Retrieved April 2, 2005, from http://freeonline.or.kr/doc/망법검토.hwp

Science, Technology, Information and Telecommunication Committee of the National Assembly (2002, December). JEONGI TONGSIN SAEOPBEOP GAEJEONG BEOPRYULAN GEOMTOBOGOSEO [A report on the Reformed Bill of Telecommunication Business Act]. Retrieved February 6, 2004, from http://freeonline.or.kr/doc/보호검토법.doc

Schiller, Herbert I. (1996). Information inequality – the deepening social crisis in America. New York: Routlege.

Seo, Soon-Bok (2003). INTERNET NAEYONGGYUJEE GWANHAN YEONGU: TONGSINPUMWIBEEOP WIHEONPANGYEOLEUL TONGHAESEO BON BEOPRIUI BALJEONGYEONGGWA [Internet-based contents regulation: focused on unconstitutional decision of Communications Decency Act]. *CYBER COMMUNICATION HAKBO, 11*, 101-141.

Shim, Young-Hee (2001). Feminism and the discourse of sexuality in Korea: Continuities and changes. *Human Studies, 24(1/2)*, 133-148.

Shim, Young-Hee (2002). CYBER SEONG POKRYEOKUI JARYUL GYUJE, NUGA JUCHEGA DOEEOYA HANA?: ISP GWANGYEJAE DAEHAN SIMCHEUNG MYEONJEOP JARYOREUL JUNGSIMEURO [Who should be the agency of self-regulation of cyber sexual violence?: Based on in-depth interviews of ISP workers]. *JEONGBOHWA JEONGCHAEK, 9(2)*, 54-74.

Shin-Yun, Donh-uk (2000, October 11). DONGSEONGAE DAMRUN, INGWONUI BADARO [Homosexuality discourse, a sea of human rights]. *THE HANKYOREH21, 329*. Retrieved April 5, 2004, from http://h21.hani.co.kr/section-021025000/2000/02102500020001011032901 4.html

Shin-Yun, Dong-uk (2001a, August 14). A, NAEGA CHEONGSONYEONYUHAEMAECHE? [Oh, is my site harmful to youth?] *THE HANKYOREH21, 372.* Retrieved July 7, 2004, from http://h21.hani.co.kr/section-021014000/2001/08/02101400020010814037 2034.html

Shin-Yun, Dong-uk (2001b, August 14). NETUI JAYU WIHYEOPHAEUN GEOMYEOLUI MINGANWA [Privatised censorship threatens freedom on the Net]. *THE HANKYOREH21, 372.* Retrieved July 7, 2004, from http://h21.hani.co.kr/section-021014000/2001/08/02101400020010814037 2015.html

Sinclair, Darren (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy*, 19(4), 529-559.

Slevin, James (2000). *The Internet and society*. Cambridge: Polity Press.

Sobel, David L. (2003, October). Internet filters and public libraries. *First Reports Vol.4, No. 2*. South Nashville, Tennessee: Vanderbilt University, First Amendment Center. Retrieved July 6, 2004, from http://www.firstamendmentcenter.org/PDF/Internetfilters.pdf

Soh, Ji-Young (2001, July 31). Homosexuals denounce online discrimination. *The Korea Times*. Retrieved July 7, 2004, from http://search.hankooki.com/times/times_view.php?terms=exzone+code%3A+kt&path=hankooki1%2Ftimes%2F200107%2Ft2001073116185740110.htm

Song, In-Geol (2001, June 14). 'INTERNET NUDE' GYOSA YEONGJANG JAECHEONGGU GEOMCHAL BINAN [Criticising the prosecution for reissuing a warrant to 'Internet nude' teacher]. *THE HANKYOREH SHINMUN*. Retrieved April 1, 2005, from http://www.hani.co.kr/section-005000000/2001/06/005000000200106142301049.html

Soular, Ray & Simpson, Wendy (1995, December). The SafeSurf Internet rating standard. Retrieved July 6, 2004, from SafeSurf Website: http://www.safesurf.com/ssplan.htm

Spaink, Karin (2003). From quill to cursor: Freedom of the media in the digital era. In OSCE (Ed.). *From Quill to Cursor: Freedom of the Media in the Digital Era* (pp. 9-30). Vienna: OSCE.

Stefik, Mark (1999). *The Internet edge: Social, legal, and technological challenges for a networked world.* Cambridge, Massachusetts: MIT Press.

Sterling, Bruce (1993). Short history of the Internet. Retrieved June 23, 2004, from http://w3.aces.uiuc.edu/AIM/scale/nethistory.html

Struck, Doug (2000, December 25). S. Koreans clash on Internet sex video. *Washington Post*. p. A35.

Sunstein, Cass R. (2001). *Republic.com*. Princeton, New Jersey: Princeton University Press.

Taggart, Stewart (2001, April 24). Questioning the Oz Net Censors. Wired News. Retrieved July 6, 2004, from http://www.wired.com/news/politics/0,1283,43182,00.html

Taylor, Greg (2001, May 5). Regulatory failure: Australia's Internet censorship regime. Retrieved July 6, 2004, from EFA Website: http://www.efa.org.au/Analysis/aba_analysis.html

Territory (2002). *The Britannica Encylopaedia* (2002 standard ed.). Chicago: Britannica.

Thornburgh, Dick & Lin, Herbert S. (Eds.) (2002). *Youth, pornography and the Internet*. Washington DC: National Academy Press.

Tierney, John (1994, January 9). Porn, the low-slung engine of progress. *The New York Times*, p. H1.

Turkle, Sherry (1997). *Life on the screen: Identity in the age of the Internet*. New York: Touchstone Books.

Ui, Hyun-Ju (2001, June 22). DONGSEONGAE SITEE CHEOLJOMANGEUL CHIDA [Stretch barbed-wire around gay sites]. *INGWON HARU SOSIK, 1880*. Retrieved July 7, 2004, from http://www.sarangbang.or.kr/

UN Population Division (2003, February 26). World population prospects: The 2002 revision: Highlights. Retrieved July 6, 2004, from http://www.un.org/esa/population/publications/wpp2002/WPP2002-HIGHLIGHTSrev1.PDF

UNICEF (2000, May 25). UN adopts two protocols for children. Retrieved March 15, 2005, from http://www.unicef.org/newsline/00pr44.htm

US Department of Commerce (1999). Falling through the Net: Defining the digital divide. Retrieved June 27, 2004, from http://www.ntia.doc.gov/ntiahome/fttn99/contents.html

US Embassy in Beijing (1998). PRC Internet: Cheaper, more popular and more Chinese. Retrieved January 17, 2002, from http://www.usembassy-china.gov/english/sandt/Inetcawb.htm

W3C (1996). Recreational Software Advisory Council launcher objective, content-labelling advisory system for the Internet. Retrieved January 6, 2002, from http://www.w3.org/PICS/960228/RSACi.html

W3C (1997a). Platform for Internet content selection. Retrieved January 6, 2002, from http://www.w3.org/PICS/

W3C (1997b). PICSRules 1.1. Retrieved February 6, 2002, from http://www.w3.org/TR/REC-PICSRules

W3C (1998). Statement on the Internet and use of PICS: Using PICS well. Retrieved January 6, 2002, from http://www.w3.org/TR/NOTE-PICS-Statement

W3C (1999). Resource Description Framework (RDF) model and syntax specification. Retrieved February 3, 2002, from http://www.w3.org/TR/1999/REC-rdf-syntax-19990222/

W3C (2000a). About the World Wide Web Consortium. Retrieved January 25, 2002, from http://www.w3.org/Consortium/

W3C (2000b). PICS frequently asked questions. Retrieved February 6, 2002, from http://www.w3.org/2000/03/PICS-FAQ/

W3C (2000c). PICS rating vocabularies in XML/RDF. Retrieved February 4, 2002, from http://www.w3.org/TR/rdf-pics

W3C (2001). Semantic activity statement. Retrieved February 14, 2002, from http://www.w3.org/2001/sw/Activity

Wallace, Jonathan (1995). An Auschwitz alphabet. Retrieved February 7, 2002, from the Ethical Spectacle Website: http://www.spectacle.org/695/ausch.html

Wallace, Jonathan (1997a). Purchase of blocking software by public libraries is unconstitutional. Retrieved September 1, 2001, from the Ethical Spectacle Website: http://www.spectacle.org/cs/library.html

Wallace, Jonathan (1997b). Why I will not rate my site. Retrieved February 7, 2002, from the Ethical Spectacle Website: http://www.spectacle.org/cda/rate.html

Wallace, Jonathan & Mangan, Mark (1997a). The Internet censorship FAQ. Retrieved March 15, 2001, from http://www.spectacle.org/freespch/faq.html

Wallace, Jonathan & Mangan, Mark (1997b). *Sex, laws, and cyberspace*. New York: Henry Holt and Company.

Waltermann, Jens & Machill, Marcel (Eds.) (2000). *Protecting our children on the Internet*. Gütersloh, Germany: Bertelsmann Foundation Publishers.

Walton, Greg (2001) China's golden shield: Corporations and the development of surveillance technology in the People's Republic of China. International Centre for Human Rights and Democratic Development: Montreal, Canada. Retrieved March 7, 2005, from http://www.ichrdd.ca/english/commdoc/publications/globalization/CGS_ENG.PDF

Wasserman, Elizabeth (1998, November 20). CDA II halted, for now. *The Industry Standard.* Retrieved May 2, 2003, from http://www.thestandard.com/article/0,1902,2626,00.html

Weil, Gordon L. (1963). *The European Convention on Human Rights: Background, development and prospects*. Leyden, Massachusetts: Sythoff.

Weinberg, Jonathan (1997). Rating the Net. *Hastings Communications and Entertainment Law Journal 19(1).* 453. Retrieved July 6, 2004, from http://www.law.wayne.edu/weinberg/rating.htm

White House (1997, July 1). The framework for global electronic commerce. The White House: Washington D.C. Retrieved March 5, 2005, from http://www.technology.gov/digeconomy/framewrk.htm

World Bank (1998). *World Development Report 1998-99: Knowledge for Development*. Oxford: Oxford University Press.

Yang, Kun (2000). The Constitutional Court and democratization. In Yoon, Dae-Kyu (Ed.) *Recent Transformations in Korean Law and Society* (pp.33-46). Seoul: Seoul National University Press.

Yoo, Cheong-Mo (2002, July 2). 'Red Devils' cheerers fascinate globe with soccer zeal, manners. *The Korea Herald.* Retrieved April 29, 2005, from http://www.koreaherald.co.kr/archives/result_contents.asp?id=200207020054

Yoon, Jae-Hee (1998). HANGUKUI OEHWANWIGI WONINGWA DAECHAEKAE GWANHAN YEONGU [A study of causes and counterpanes for IMF period in Korea]. *SAHOE GWAHAK YEONGU 6.* 149-171.

Youm, Kyu-Ho (2001). The Constitutional Court and freedom of expression. *Journal of Korean Law, 1(2)*, 37-70.

Youm, Kyu-Ho (2002). Freedom of expression and the law: Rights and responsibilities in South Korea. *Stanford Journal of International Law, 38*, 123-151.

Zakon, Robert H. (2004). Hobbes' Internet Timeline v7.0. Retrieved June 23, 2004, from http://www.zakon.org/robert/internet/timeline/

Zittrain, Jonathan & Edelman, Benjamin (2003). Empirical Analysis of Internet Filtering in China. Retrieved November 7, 2003, from Harvard University, Berkman Center Website: http://cyber.law.harvard.edu/filteirng/china/

APPENDIX A

Technical Specifications of Reviewed Filtering Software

Cyber Patrol

Version	Cyber Patrol 5.0
Producer	SurfControl (http://www.cyberpatrol.com)
Cost	£39.95 (including 12month subscription)
Subscription	£39.95 for additional 12 month subscription
System Requirements	[Windows] Operating System: Windows® 95, 98, ME, NT 4.0, 2000 Pro / Processor 486 or greater / Memory: 32 MB / Hard disk space: 30 MB [Macintosh] Operating System: Macintosh® System 7.1 through 9.x / Processor: 68020 or higher / Memory: 32 MB / Hard disk space: 20 MB
Filtering Coverage	Websites / Newsgroups / Internet Relay Chat / Applications
Filtering Methods	Blacklist / Whitelist / Keyword / Time Control
Filter List	Editable / Not viewable
PICS	Compliant
Classification	12 Categories Violence/Profanity, Partial Nudity, Full Nudity, Sexual Acts, Gross Depictions, Intolerance, Satanic/Cult, Drugs/Drug Culture, Militant/Extremist, Sex Education, Questionable/Illegal & Gambling, Alcohol & Tobacco,
Filter List Updates	Daily
Multi-Profiles	Available (up to 9 profiles)

Cyber Sentinel

Version	Cyber Sentinel 2.0 Home Edition
Producer	Security Software Systems, Inc. (http://www.securitysoft.com)
Cost	£ 46.94
Subscription	None
System Requirements	Operating System: Windows® 95, 98, ME, NT 4.0, 2000 Pro / Processor: 166MHz Pentium or compatible / Memory: 32 MB or higher / Hard disk space: 20 MB or higher
Filtering Coverage	Websites / FTP sites / E-mail (inbound and outbound) / Newsgroups / Internet Relay Chat / ICQ[1] Chat / TELNET / AOL Instant Messenger and AOL TCP/IP logins / CompuServe TCP/IP logins / MSN Messenger
Filtering Methods	Blacklist / Whitelist / Keyword / Time Control
Filter List	Editable / Not viewable
PICS	Not compliant
Classification	Unknown
Filter List Updates	None
Multi-Profiles	Not available

[1] ICQ ("I Seek You") is a program you can download that will let you know when friends and contacts are also online on the Internet. ICQ allows you to page them, chat with them, and initiate and participate in PC-to-PC calls, PC-to-phone and phone-to-phone calling cards calls. Like AOL's Instant Messenger (AIM), in order to use ICQ, both parties must have downloaded the program.

CYBERsitter

Version	CYBERsitter 2001
Producer	Solid Oak Software, Inc. (http://www.solidoak.com)
Cost	$39.95 (USD)
Subscription	Free
System Requirements	Operating System: Windows® 95, 98, ME, NT 4.0, 2000, XP / Hard disk space: 2 MB / Web-browser: Any Browser
Filtering Coverage	Websites / FTP sites / E-mail / Newsgroups / ICQ Chat / AOL Instant Messenger
Filtering Methods	Blacklist / Whitelist / Keyword / Time Control
Filter ListEditable	/ Not viewable
PICS	Compliant
Classification	30 categories (5 Default Categories and 25 Optional Categories)
	Default: Adult/Sexually Oriented, Illegal Activities/Drugs, Adult/Violence, Hate/Intolerance, Illegal Guns/Violence
	Optional: Gay/Lesbian Topics, Cults/Occult, Violent Games, Tobacco/Alcohol, Gambling Sites, Banner Ads, Legal Guns/Weapons, Personal Ads, Tattoo/Piercing, Warez/Hacker Sites, On-line Chat, Shareware Sites, Financial Sites, Illegal MP3 Files, Popup Ad Windows, Sports, Game Sites, On-line Auctions, TV/Entertainment, Movie Sites, Wrestling, Job search, Fee E-Mail Sites, Pokemon Site, Astrology/Fortune Telling
Filter List Updates	Periodical
Multi-Profiles	Not available

Cyber Snoop

Version	Cyber Snoop 4.0
Producer	Pearl Software, Inc. (http://www.pearlsw.com/)
Cost	$49.95 (USD)
Subscription	None
System Requirements	
	Operating System: Windows® 95, 98, ME, 2000, NT, or XP
	Processor: 486 or higher processor / Memory: 4 MB
	Hard disk space: 20 MB
Filtering Coverage	
	Websites / FTP sites / E-mail / Web-based E-mail / Newsgroups / IRC Chat Rooms / ICQ Instant Messenger / AOL Instant Messenger
Filtering Methods	
	Blacklist / Whitelist / Keyword / Time Control
Filter List	Editable / Viewable
PICS	Compliant
Classification	None
Filter List Updates	None (The "Starter List" is provided via e-mail by a user's request.)
Multi-Profiles	Available

Net Nanny

Version	Net Nanny 4
Producer	Net Nanny Software Inc. (http://www.netnanny.com)
Cost	£34.99
Subscription	Free
System Requirements	
	Operating System: Windows® 95, 98, 2000, NT 4.0 / Processor: Pentium or higher processor / Memory: 32 MB / Hard disk space: 50 MB
Filtering Coverage	
	Website / Newsgroups / IRC chat rooms
Filtering Methods	
	Blacklist / Whitelist / Keyword / Time Control
Filter List	Editable / Viewable
PICS	Compliant
Classification	5 Categories
	Sexually Explicit, Hate, Violence, Crime, Drugs
Filter List Updates	Daily
Multi-Profiles	Available (up to 12 profiles)

Norton Internet Security

Version	Norton Internet Security 2002
Producer	Symantec (http://www.symantec.com)
Cost	£41.86 (including 12month subscription)
Subscription	$16.95(USD) for additional 12 month subscription
System Requirements	Operating System: Windows® 98, ME, NT 4.0, 2000, XP / Processor: Pentium 150MHz or higher / Memory: 32MB, 64MB for NT and 2000, 128MB for XP / Hard disk space: 90MB with Parental Control Web browser: Internet Explorer 4.01 Service Pack 1 or higher
Filtering Coverage	Websites / Applications
Filtering Methods	Blacklist / Whitelist
Filter List	Editable / Not viewable
PICS	Not compliant
Classification	31 Categories Adult Humour, Alcohol-Tobacco, Anonymous Proxies, Crime, Drugs/Advocacy, Drugs/Non-medical, Entertainment/Games, Entertainment/Sports, Finance, Gambling, Humour, Interactive/Chat, Interactive/Mail, Intolerance, Job Search, News, Occult/New Age, Prescription Medicine, Real Estate, Religion, Sex/Acts, Sex/Attire, Sex/Nudity, Sex/Personals, Sex Education/Basic, Sex Education/Advanced, Sex Education/Sexuality, Travel, Vehicles, Violence, Weapons
Filter List Updates	Every two weeks
Multi-Profiles	Available (unlimited number of profiles)

N2H2

Version	N2H2 1.0
Producer	N2H2 (http://www.n2h2.com)
Cost	$ 39.95 (USD) including 12month subscription and upgrades
Subscription	$ (USD) for additional 12 month subscription and upgrades
System Requirements	Operating System: Windows® 95, 98, 2000, NT 4.0 with service pack 4 or later, / Processor: 486 or higher / Memory: 16MB / Hard disk space: 3 MB / Web-browser: Internet Explorer 4.0 or higher, Netscape Navigator 3.0 or higher, Opera 3.62 or higher, NeoPlanet 5.1 or higher, AOL 4.0 or higher, CompuServe 2, Earthlink 2.3 or higher
Filtering Coverage	Websites
Filtering Methods	Blacklist / Whitelist
Filter ListEditable /	Not viewable
PICS	Not compliant
Classification	36 categories and 6 exceptional categories Adults Only, Alcohol, Auction, Chat, Drugs, Electronic Commerce, Employment Search, Free Mail, Free Pages, Gambling, Games, Hate/Discrimination, Illegal, Jokes, Lingerie, Message/Bulletin Boards, Murder/Suicide, News, Nudity, Personal Information, Personals, Pornography, Profanity, Recreation/Entertainment, School Cheating Information, Search Engines, Search Terms, Sex, Sports, Stocks, Swimsuits, Tasteless/Gross, Tobacco, Violence, Weapons *Exceptions*: Education, For Kids, History, Medical, Moderated, Text/Spoken Only
Filter List Updates	Daily
Multi-Profiles	Available

Pure Sight

Version	Pure Sight 2.5
Producer	iCognito (Intelligent Content Recognition / http://www.puresight.com)
Cost	$ 39.95 (USD)
Subscription	None
System Requirements	Operating System: Windows® 98, ME, NT 4.0 with service pack 4 or later, 2000 / Processor: 486 or higher / Hard disk space: 8 MB / Web-browser: Any Web browser
Filtering Coverage	Websites, FTP sites
Filtering Methods	Artificial Intelligent engine / Blacklist / Whitelist / User-defined Control
Filter List	Editable / Not viewable
PICS	Compliant
Classification	2 Categories: Sex / Gambling
Filter List Updates	None
Multi-Profiles	Not available

We-Blocker

Version	We-Blocker 2.0.1
Producer	We-WebCorp.com (http://www.we-blocker.com/)
Cost	Free
Subscription	Free
System Requirements	Operating System: Windows® 95/98/2000/ME/NT 4.0 / Processor: 120MHz Pentium / Memory: 32MB / Hard disk space: 5 MB / Web-browser: Microsoft Internet Explorer 3.02 or Netscape Navigator 3.02 or better
Filtering Coverage	Websites
Filtering Methods	Blacklist / Whitelist / Keyword
Filter List	Editable / Not viewable
PICS	Not compliant
Classification	7 Categories Pornography, Violence, Drugs and Alcohol, Gambling, Hate Speech, Adult Subjects, Weaponry
Filter List Updates	Daily
Multi-Profiles	Available

X-stop

Version	X-stop v3.04DX
Producer	8e6 Technologies (http://www.xstop.com/)
Cost	$ 60 (USD) for one-year commitment
Subscription	Free
System Requirements	Operating System: Windows® 95, 98 and NT / Processor: Pentium / Memory: 32 MB recommended / Hard disk space: 50 MB
Filtering Coverage	Websites / FTP sites / Newsgroups / Phone number
Filtering Methods	Blacklist / Keyword
Filter List	Editable / Not viewable
PICS	Not compliant
Classification	34 categories Alcohol, Alternative Journals, Anarchy, Automobile, Banner Ads, Chat, Criminal Skills, Cults/Gothic, Drugs, Employment, Entertainment, Financial, Free Hosts, Gambling, Games, Hate & Discrimination, Humor, Lifestyle, Magazines, News, Obscene/Tasteless, Opinion/Politics and Religion, Personal/Dating, PG-17, Pornography, R-rated, Search Engines, Self-Help, Shopping, Sports, Tickets, Travel, Web-based E-mail, Web-based Proxies Anonymizers, Web-based Newsgroups
Filter List Updates	Daily
Multi-Profiles	Not available

APPENDIX B

Comparative Table: Technical Specifications of Reviewed Filtering Software

Note: ●=Yes, ✘=No, D=Daily, P=Periodical, 2W=Every two weeks, N=None, UL=Unlimited, UN=Unknown

	Cyber Patrol	Cyber Sentinel	CYBERsitter	Cyber Snoop	Net Nanny	Norton IS	N2H2	Pure Sight	We-Blocker	X-Stop
Price	£39.95	£46.94	$39.95	$49.95	£34.99	£41.86	$39.95	$39.95	Free	$60.00
Subscription	£39.95	—	Free	—	$16.95	Free	—	—	Free	Free
Downloadable	●	●	●	●	●	●	●	●	●	●
Free trial available	●	●	●	●	✘	✘	●	●	Free	●
Filtering Coverage										
Websites	●	●	●	●	●	●	●	●	●	●
FTP sites	✘	●	●	●	✘	✘	✘	●	✘	●
E-mail	✘	●	●	●	✘	✘	✘	✘	✘	✘
Newsgroups	●	●	●	●	●	✘	✘	✘	✘	●
Chat	●	●	●	●	●	✘	✘	✘	✘	✘
Applications	●	●	✘	✘	✘	●	✘	✘	✘	✘
Filtering Methods										
Blacklist	●	●	●	●	●	●	●	●	●	●
Whitelist	●	●	●	●	●	●	●	●	●	✘
Keyword	●	●	●	●	●	✘	●	●	●	●
Time control	●	●	●	●	●	✘	✘	✘	✘	✘
PICS-compliant	●	✘	●	●	●	✘	✘	●	✘	✘
Reporting										
Report	●	●	●	●	●	●	✘	●	●	✘
E-mail report	✘	●	●	✘	✘	✘	✘	✘	✘	✘
Local warning	●	●	✘	●	●	●	●	●	●	●
Customisability										
Filter List editable	●	●	●	●	●	●	●	●	●	●
Filter List viewable	✘	✘	✘	●	●	✘	✘	✘	✘	✘
Usability										
Operating System: Windows	●	●	●	●	●	●	●	●	●	●
Operating System: Mac	●	✘	✘	✘	✘	✘	✘	✘	✘	✘
Uninstaller	●	●	●	●	✘	●	●	✘	●	✘
Graphical scheduling	●	●	✘	●	●	✘	✘	✘	●	✘
Multi-User accounts	●	✘	✘	●	●	●	●	✘	●	✘
Number of accounts available	10	—	—	UL	12	UL	UN	—	UN	—
Account setup wizard	✘	✘	✘	✘	●	●	●	✘	✘	✘
Filter List updates	D	N	P	N	D	2W	D	N	D	D
Number of categories	12	—	30	—	5	31	40	2	7	34

APPENDIX C

Technical Review: 10 Examples of Commercial Filtering Software:
The List of the Sample Websites and the Detailed Results

Notes: ▩ = Blocking **CP**=Cyber Patrol, **CSE**=Cyber Sentinel, **CSI**=CYBERsitter, **CSN**=Cyber Snoop, **NN**=Net Nanny, **NIS**=Norton Internet Security, **NH**=N2H2, **PS**=Pure Sight, **WB**=We-Blocker, **XS**=X-Stop

Alcohol (keyword: alcohol)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	The National Clearinghouse for Alcohol and Drug Information, US http://www.health.org/										
02	The U.S. Bureau of Alcohol, Tobacco and Firearms http://www.atf.treas.gov/index.htm										
03	Alcohol Concern http://www.alcoholconcern.org.uk/										
04	The National Institute on Alcohol Abuse and Alcoholism, US http://www.niaaa.nih.gov/										
05	Alcohol and Alcoholism (Oxford Journals online) http://alcalc.oupjournals.org/										
06	The Higher Education Center for Alcohol and Other Drug Prevention, US http://www.edc.org/hec/										
07	Alcohol: Problems and Solutions http://www2.potsdam.edu/alcohol-info/default.html										
08	Center of Alcohol Studies http://www.rci.rutgers.edu/~cas2/										
09	Brown University, Center for Alcohol and Addictions Studies http://center.butler.brown.edu/										
10	Alcohol Advisory Council of New Zealand http://www.alcohol.org.nz/about/home.html										
11	The National Organization on Fetal Alcohol Syndrome, US http://www.nofas.org/										
12	The National Association of State Alcohol and Drug Abuse Directors http://www.nasadad.org/										
13	Fetal Alcohol And Drug Unit, University of Washington http://depts.washington.edu/fadu/										
14	College Alcohol Study, Harvard School of Public Health http://www.hsph.harvard.edu/cas/										
15	California Department of Alcohol and Drug Programs http://www.adp.cahwnet.gov/										
16	International Council on Alcohol and Addictions http://www.icaa.de/index2.htm										
17	Alcohol Studies Database http://www.scc.rutgers.edu/alcohol_studies/										
18	Internet Alcohol Recovery Center, University of Pennsylvania http://www.uphs.upenn.edu/~recovery/										
19	Facts on Tap: Alcohol and your college experience http://www.factsontap.org/										
20	The Alcohol and Temperance History Group http://www.athg.org/										

Table AC1

Crime (keyword: crime)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	The National Crime Prevention Council http://www.ncpc.org/										
02	Crime.com http://www.crime.com/										
03	Office for Victims of Crime http://www.ojp.usdoj.gov/ovc/										
04	The United Nations Crime and Justice Information Network http://www.uncjin.org/										
05	Organized Crime (A Crime Statistics Site) http://www.crime.org/homepage.html										
06	The Crime Library http://www.crimelibrary.com/										
07	Computer Crime and Intellectual Property Section of the Criminal Division of the US Department of Justice http://www.cybercrime.gov/										
08	Crime Scene Evidence Files http://www.crimescene.com/										
09	Crime Stoppers International http://www.c-s-i.org/										
10	Crime Reduction http://www.crimereduction.gov.uk/										
11	About Crime and Punishment http://crime.about.com/										
12	Crime Magazine http://crimemagazine.com/										
13	The National Center for Victims of Crime http://www.ncvc.org/										
14	Homestore.com http://www.homefair.com/homefair/calc/crime.html										
15	The Crime Mapping Research Center http://www.ojp.usdoj.gov/cmrc/										
16	The National Crime Prevention Centre, Canada http://www.crime-prevention.org/index_ncpc.html										
17	Youth Crime Watch America http://www.ycwa.org/										
18	Crime Spider http://www.crimespider.com/										
19	Sisters in Crime http://www.sistersincrime.org/										
20	Internet Crime Archives http://www.mayhem.net/Crime/archives.html										

Table AC2

Drugs (keyword: drug)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	RxList, The Internet drug Index http://www.rxlist.com/										
02	Clubdrugs.org —A service of the National Institute on Drug Abuse, US http://www.clubdrugs.org/										
03	The European Monitoring Centre for Drugs and Drugs Addiction http://www.emcdda.org/										
04	World Wide Drugs http://community.net/~neils/new.html										
05	Stop drugs http://www.stopdrugs.org/										
06	London Drugs http://www.londondrugs.com/										
07	Drugs.com (Drug Information Online) http://www.drugs.com/										
08	Longs Drugs http://www.longs.com/										
09	Drugs, Brains and Behavior http://www.rci.rutgers.edu/~lwh/drugs/										
10	The National Institute on Drug Abuse, US http://www.nida.nih.gov/DrugAbuse.html										
11	U.S. Drug Enforcement Administration http://www.usdoj.gov/dea/concern/concern.htm										
12	The Indiana Prevention Resource Center at Indiana University http://www.drugs.indiana.edu/										
13	Doctor's Guide: New Drugs or Indications http://www.pslgroup.com/NEWDRUGS.HTM										
14	The U.S. Department of Justice Bureau of Justice Statistics http://www.ojp.usdoj.gov/bjs/drugs.htm										
15	The World Health Organization / Essential Drugs and Medicines Policy http://www.who.int/medicines/										
16	Scottish Drugs Forum http://www.sdf.org.uk/										
17	Current Drugs http://www.current-drugs.com/										
18	The National Criminal Justice Reference Service / Drugs And Crime http://virlib.ncjrs.org/DrugsAndCrime.asp										
19	Home Office (UK) Drugs Prevention http://www.homeoffice.gov.uk/atoz/drugs.htm										
20	The National Drugs Helpline (UK) http://www.ndh.org.uk/										

Table AC3

Gambling (keyword: gambling)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	AnteUp GamblingLinks.com http://gamblinglinks.com/										
02	Gambling.com http://www.gambling.com/										
03	411Vegas http://www.411vegas.com/										
04	The National Council on Problem Gambling, US http://www.ncpgambling.org/										
05	Online Gambling Sites http://www.1-online-gambling-sites.com/										
06	The National Gambling Impact Study Commission, US http://www.ngisc.gov/										
07	Exclamation Online Gambling http://www.exclamation-online-gambling.com/										
08	Gamblinglinks http://gamblinglinks.net/										
09	Online Casinos Gambling http://top-casino-gambling.com/										
10	About.com — Casino Gambling http://casinogambling.about.com/										
11	4 Online Casino Gambling http://www.4onlinecasinogambling.com/										
12	Gambling-casino-world.com http://gambling-casino-world.com/										
13	Online Gambling Information & Books http://www.online-gambling-books.com/										
14	Online Gambling Club http://www.onlinegamblingclub.com/										
15	Gambling Times http://www.gamblingtimes.com/										
16	Internet Casino Gambling and Slots http://www.a-internet-online-casino-gambling.com/										
17	Online Casino Gambling http://www.exclamationpoint-online-casino-gambling.com/										
18	BizMove.com / Gambling http://www.bizmove.com/topics/gambling.htm										
19	The Responsible Gambling Council, Canada http://www.responsiblegambling.org/index-regular.html										
20	Internet Gambling Bonus http://internet-gambling-bonus.com/										

Table AC4

Gay/Lesbian (keyword: gay)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	Gay.com UK http://uk.gay.com/										
02	The National Gay and Lesbian Task Force, US http://www.ngltf.org/										
03	The Gay Financial Network http://www.gfn.com/										
04	The Gay Lesbian and Straight Education Network http://www.glsen.org/templates/index.html										
05	The Gay & Lesbian Alliance Against Defamation http://www.glaad.org/org/index.html										
06	The Gay Men's Health Crisis http://www.gmhc.org/										
07	The International Gay and Lesbian Human Rights Commission http://www.iglhrc.org/										
08	Gay Wired http://www.gaywired.com/										
09	The International Lesbian and Gay Association http://www.ilga.org/										
10	The Federation Of Gay Games http://www.gaygames.com/en/										
11	The Gay and Lesbian Medical Association http://www.glma.org/home.html										
12	The National Lesbian & Gay Journalists Association http://www.nlgja.org/										
13	The Gay & Lesbian Hotline http://www.glnh.org/										
14	GayUniverse http://www.gayuniverse.com/										
15	Gay-Lesbian Politics and Law WWW and Internet Resources http://www.indiana.edu/~glbtpol/										
16	Gay Today http://www.gaytoday.badpuppy.com/default2.asp										
17	Russian Gays http://www.gay.ru/english/										
18	Gay Games VI Sport & Cultural Festival, Sydney 2002 http://www.sydney2002.org.au/frameset.asp										
19	GayCanada http://www.gaycanada.com/index.php										
20	Gay Parent http://www.gayparentmag.com/										

Table AC5

Hate (keyword: nazi)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	Anti-Nazi League Campaigns http://www.anl.org.uk/campaigns.htm										
02	NOVA Online Decoding Nazi Secrets http://www.pbs.org/wgbh/nova/decoding/										
03	Documentary resources on the Nazi genocide http://www.anti-rev.org/										
04	The American Nazi Party http://www.americannaziparty.com/										
05	The Avalon Project Nazi-Soviet Relations 1939-1941 http://www.yale.edu/lawweb/avalon/nazsov/nazsov.htm										
06	Nazi Propaganda (1933-1945) http://www.calvin.edu/academic/cas/gpa/ww2era.htm										
07	Nazi & Soviet Art http://www.primenet.com/~byoder/artofnz.htm										
08	Libertarian National Socialist Green Party http://www.nazi.org/										
09	1936 Olympics http://www.ushmm.org/olympics/										
10	Law-Related Resources on Nazi Gold and Other Holocaust Assets http://www.lib.uchicago.edu/~llou/nazigold.html										
11	Nazi Lauck NSDAP/AO http://www.nazi-lauck-nsdapao.com/										
12	Nazi War Criminal Records Interagency Working Group http://www.nara.gov/iwg/										
13	Medical Experiments of the Holocaust and Nazi Medicine http://www.remember.org/educate/medexp.html										
14	The Nazi Occupation of Poland http://www.ibiscom.com/poland.htm										
15	Modern World History Nazi Germany http://www.bbc.co.uk/education/modern/nazi/nazihtm.htm										
16	The Nazism Exposed Project http://www.ekran.no/html/nazismexposed/										
17	Financial compensation for Nazi slave laborers http://www.religioustolerance.org/fin_nazi.htm										
18	The Nazi Doctors http://members.aol.com/poloboy02/nazi1.htm										
19	Nazi Persecution of Homosexuals http://members.aol.com/dalembert/lgbt_history/nazi_biblio.html										
20	World War II Nazi Holocaust Hitler Children's Home Page http://home.online.no/~kluwer/										

Table AC6

Pornography (keyword: porn)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	PornResource.com http://www.pornresource.com/										
02	Adult Sites Against Child Pornography http://www.asacp.org/										
03	LEGO PORN http://www.asacp.org/										
04	Free Extreme Adult Entertainment http://www.cybererotica.com/free-sites.html										
05	Mega porn links http://www.mega-porn-links.com/										
06	Porn-Free.org http://www.porn-free.org/										
07	MyPorn.com http://www.myporn.com/										
08	Quality Porn Links http://www.penisbot.com/										
09	Here Is The Porn http://www.hereistheporn.com/main/										
10	Free Porn List http://www.freepornlist.com/										
11	Porn-Station http://www.porn-station.com/Directory/New/										
12	Porn Passwords http://www.porn-passwords.net/										
13	Asian Spreads http://www.japanese-porn.org/										
14	Hosts for Porn http://hosts4porn.com/										
15	XXX Asian Porn Pics http://www.xxxasianporn.net/										
16	Free Daily Pics http://www.karasxxx.com/potd/newmainpotd.shtml?tekiegeek:pd										
17	Report Child Porn to Government Agencies http://www.reportchildporn.com/										
18	TokyoPorn.com http://www.tokyoporn.com/										
19	Legal Porn http://www.legalporn.com/										
20	We Love Free Porn http://www.welovefreeporn.com/										

Table AC7

Sex (keyword: sex)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	Safersex.org http://www.safersex.org/										
02	SEX.ETC http://www.sxetc.org/										
03	Salon.com Sex http://www.salon.com/sex/										
04	HBO Sex and the City http://www.hbo.com/city/										
05	It's Your (Sex) Life http://www.itsyoursexlife.com/										
06	Sex, Censorship, and the Internet http://www.eff.org/CAF/cafuiuc.html										
07	Stop Sex Offenders! http://www.stopsexoffenders.com/										
08	All About Sex Discussion Web http://www.allaboutsex.org/										
09	The Sex Education Web Circle http://www.sexuality.org/wc/										
10	San Francisco Sex Information http://www.sfsi.org/										
11	Center for Sex Offender Management http://www.csom.org/										
12	Sex Scrolls http://www.sexscrolls.com/										
13	American Association of Sex Educators, Counselors, and Therapists http://www.aasect.org/										
14	Sex books (book reviews) http://dannyreviews.com/s/sex.html										
15	Sacred Sex http://www.luckymojo.com/sacredsex.html										
16	The Kinsey Institute for Research in Sex, Gender, and Reproduction http://www.indiana.edu/~kinsey/										
17	Sex Therapy Online http://www.sexology.org/										
18	Jane's net sex guide http://www.janesguide.com/										
19	The Sex Thermometer http://www.sexthermometer.com/										
20	Sex and Love Addicts Anonymous http://www.slaafws.org/										

Table AC8

Tobacco (keyword: cigarette)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	The Cigarette Papers http://www.library.ucsf.edu/tobacco/cigpapers/										
02	CigaretteLitter.Org http://www.cigarettelitter.org/										
03	Cigarette Racing Team http://www.cigaretteracing.com/										
04	Cigarette.com http://www.cigarette.com/										
05	NOVA Online / Search for a Safe Cigarette http://www.pbs.org/wgbh/nova/cigarette/										
06	Lung Cancer and Cigarette Smoking Web Page http://ourworld.compuserve.com/homepages/LungCancer/										
07	Cigarette Anyone http://www.emphysema.net/my.html										
08	The No Smoke Cafe http://www.clever.net/chrisco/nosmoke/stop.html										
09	Cigarette Network http://www.cigarettenetwork.com/index.html										
10	Cigarette Cards 101 http://home.earthlink.net/~cardking/										
11	Cigarette Pack Collectors Association http://hometown.aol.com/cigpack/index.html										
12	Discount Cigarette Shop http://www.cigaretteshop.com/										
13	Cigarette Outlet http://www.cigaretteoutlet.com/										
14	Cigarette Modification Products http://www.quitsmoking.com/cigarettemodprods.htm										
15	Fact Sheet – Cigarette Smoking http://www.well.com/user/woa/fssmoke.htm										
16	Discount Cigarette Outlet http://www.discountcigarette.com/										
17	German Cards http://www.germancards.com/										
18	CDC Media Relations Facts About Cigarette Mortality http://www.cdc.gov/od/oc/media/fact/cigmortl.htm										
19	The Cigarette Store http://www.cigstore.com/										
20	Fire Safe Cigarette http://www.burnfoundation.org/firesafecig.html										

Table AC9

Violence (keyword: gun)		CP	CSE	CSI	CSN	NN	NIS	NH	PS	WB	XS
01	Gun Owners of America http://www.gunowners.org/										
02	Coalition to Stop Gun Violence http://www.gunfree.org/										
03	E-Gun http://www.e-gun.net/										
04	Student Pledge Against Gun Violence http://www.pledge.org/										
05	GunHoo Gun Pages Central Firearms Links http://www.gunsgunsguns.com/gunhoo/										
06	Women Against Gun Control http://www.wagc.com/										
07	The Brady Campaign to Prevent Gun Violence http://www.bradycampaign.org/										
08	The Gun Room http://www.doublegun.com/										
09	GunBroker.com Online Gun Auction http://www.gunbroker.com/										
10	Gun Owners of California http://www.gunownersca.com/										
11	Gun Violence Home Page http://www.jointogether.org/gv/										
12	Gun Free Kids http://www.gunfreekids.org/										
13	GunTruths—the truth about guns http://www.guntruths.com/										
14	Dixie Gun Works http://www.dixiegunworks.com/										
15	Americans for Gun Safety http://ww2.americansforgunsafety.com/										
16	Gun Laws, Gun Control and Gun Rights http://ww2.americansforgunsafety.com/										
17	The World Wide Web Gun Defense Clock http://www.pulpless.com/gunclock/										
18	Ithaca Gun Company http://www.ithacagun.com/										
19	Gunindex.com http://www.igun.com/										
20	Gun Control vs. Gun Rights The Issue http://www.opensecrets.org/news/guns/										

Table AC10

APPENDIX D

The SafeSurf SS~~ Rating Standard

The SafeSurf SS~~ Rating Standard

Designed with input from thousands of parents and Net citizens to empower each family to make informed decisions concerning accessibility of online content.

Section One: Adult Themes with Caution Levels

SS~~000. Age Range

1) All Ages
2) Older Children
3) Teens
4) Older Teens
5) Adult Supervision Recommended
6) Adults
7) Limited to Adults
8) Adults Only
9) Explicitly for Adults

Section One: Adult Themes with Caution Levels

SS~~001. Profanity

1) Subtle Innuendo
Subtly Implied through the use of Slang
2) Explicit Innuendo
Explicitly implied through the use of Slang
3) Technical Reference
Dictionary, encyclopedic, news, technical references
4) Non-Graphic-Artistic
Limited non-sexual expletives used in a artistic fashion
5) Graphic-Artistic
Non-sexual expletives used in a artistic fashion
6) Graphic
Limited use of expletives and obscene gestures
7) Detailed Graphic
Casual use of expletives and obscene gestures.
8) Explicit Vulgarity
Heavy use of vulgar language and obscene gestures. Unsupervised Chat Rooms.
9) Explicit and Crude
Saturated with crude sexual references and gestures. Unsupervised Chat Rooms.

SS~~002. Heterosexual Themes
1) Subtle Innuendo
Subtly Implied through the use of metaphor
2) Explicit Innuendo
Explicitly implied (not described) through the use of metaphor
3) Technical Reference
Dictionary, encyclopedic, news, medical references
4) Non-Graphic-Artistic
Limited metaphoric descriptions used in an artistic fashion
5) Graphic-Artistic
Metaphoric descriptions used in an artistic fashion
6) Graphic
Descriptions of intimate sexual acts
7) Detailed Graphic
Descriptions of intimate details of sexual acts
8) Explicitly Graphic or Inviting Participation
Explicit Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.
9) Explicit and Crude or Explicitly Inviting Participation
Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.

SS~~003. Homosexual Themes
1) Subtle Innuendo
Subtly Implied through the use of metaphor
2) Explicit Innuendo
Explicitly implied (not described) through the use of metaphor
3) Technical Reference
Dictionary, encyclopedic, news, medical references
4) Non-Graphic-Artistic
Limited metaphoric descriptions used in an artistic fashion
5) Graphic-Artistic
Metaphoric descriptions used in an artistic fashion
6) Graphic
Descriptions of intimate sexual acts
7) Detailed Graphic
Descriptions of intimate details of sexual acts
8) Explicitly Graphic or Inviting Participation
Explicit descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or Newsgroups.
9) Explicit and Crude or Explicitly Inviting Participation
Profane Graphic Descriptions of intimate details of sexual acts designed to arouse. Inviting interactive sexual participation. Unsupervised Sexual Chat Rooms or

Newsgroups.

SS~~004. Nudity
1) Subtle Innuendo
Subtly Implied through the use of composition, lighting, shaping, revealing clothing, etc.
2) Explicit Innuendo
Explicitly implied (not shown) through the use of composition, lighting, shaping or revealing clothing
3) Technical Reference
Dictionary, encyclopedic, news, medical references
4) Non-Graphic-Artistic
Classic works of art presented in public museums for family viewing
5) Graphic-Artistic
Artistically presented without full frontal nudity
6) Graphic
Artistically presented with frontal nudity
7) Detailed Graphic
Erotic frontal nudity
8) Explicit Vulgarity
Pornographic presentation, designed to appeal to prurient interests.
9) Explicit and Crude
Explicit pornographic presentation

SS~~005. Violence
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Inviting Participation in Graphic Interactive Format
9) Encouraging Personal Participation, Weapon Making

SS~~006. Sex, Violence, and Profanity
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Explicit Vulgarity
9) Explicit and Crude

SS~~007. Intolerance - (Intolerance of another person's racial, religious, or gender backround)
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Literary
5) Graphic-Literary
6) Graphic Discussions
7) Endorsing Hatred
8) Endorsing Violent or Hateful Action
9) Advocating Violent or Hateful Action

SS~~008. Glorifying Drug Use
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Simulated Interactive Participation
9) Soliciting Personal Participation

SS~~009. Other Adult Themes
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Reference
4) Non-Graphic-Artistic
5) Graphic-Artistic
6) Graphic
7) Detailed Graphic
8) Explicit Vulgarity
9) Explicit and Crude

SS~~00A. Gambling
1) Subtle Innuendo
2) Explicit Innuendo
3) Technical Discussion
4) Non-Graphic-Artistic, Advertising
5) Graphic-Artistic, Advertising
6) Simulated Gambling
7) Real Life Gambling without Stakes
8) Encouraging Interactive Real Life Participation with Stakes
9) Providing Means with Stakes

APPENDIX E

The Statistics of ICEC Deliberations (1997-2002)

January 2002—December 2002

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	5,649	2,618	9	61	2,398	150
Defamation / Privacy Violation	116	21	17	4	0	0
Speculative spirit promotion / Pyramid	422	115	58	22	27	8
Wild rumour	5	0	0	0	0	0
Anti-nation	69	3	0	3	0	0
Fraudulent election	812	0	0	0	0	0
Injustice Advertisement	3	2	0	2	0	0
Obscenity / Violence Text	990	531	315	85	108	23
Obscenity / Violence Sound	5	3	3	0	0	0
Obscenity / Violence material sale	383	82	16	23	19	24
Obscenity / Violence material purchase	1	0	0	0	0	0
Obscenity / Violence material exchanging	68	49	5	43	1	0
Leading unhealthy meeting	531	350	155	136	28	31
Unhealthy chatting	659	599	10	559	28	2
Introducing a place of obscene material	4,531	773	349	289	122	13
Verbal violence	209	77	2	55	19	1
Prostitution	1	0	0	0	0	0
Obscene still image	8,792	3,362	1,708	56	2	1,596
Violence still image	59	21	9	3	0	9
Obscene movie	3,872	2,075	1,056	5	1	1,013
Violence movie	25	3	1	0	0	2
Obscene game	103	74	34	23	0	17
Violence game	58	0	0	0	0	0
Etc. / Out of classification	3,269	275	18	65	119	73
Non-deliberation subject	1,589	0	0	0	0	0
Total	32,221	11,033	3,765	1,434	2,872	2,962

January 2001—December 2001

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	6,581	6,290	819	254	4,137	1,080
Defamation / Privacy Violation	112	18	15	2	0	1
Speculative spirit promotion / Pyramid	139	34	1	0	32	1
Wild rumour	30	28	28	0	0	0
Anti-nation	0	0	0	0	0	0
Injustice Advertisement	1	0	0	0	0	0
Obscenity / Violence Text	1,299	943	602	232	20	89
Obscenity / Violence Sound	1	0	0	0	0	0
Obscenity / Violence material sale	633	462	16	50	145	251
Obscenity / Violence material purchase	65	59	11	48	0	0
Obscenity / Violence material exchanging	621	594	14	577	3	0
Leading unhealthy meeting	1,387	1,098	94	230	637	137
Unhealthy chatting	3,503	3,154	6	3,101	46	1
Introducing a place of obscene material	301	102	27	50	21	4
Verbal violence	420	264	42	219	2	1
Prostitution	0	0	0	0	0	0
Obscene still image	5,698	5,051	3,352	250	27	1,422
Violence still image	134	117	80	11	0	26
Obscene movie	1,928	1,761	1,109	62	1	589
Violence movie	27	23	8	7	0	8
Obscene game	372	318	127	134	0	57
Violence game	5	0	0	0	0	0
Etc. / Out of classification	1,935	1,186	734	96	9	347
Non-deliberation subject	18	0	0	0	0	0
Total	25,210	21,502	7,085	5,323	5,080	4,014

January 2000—December 2000

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	5,872	4,822	137	2,270	2,260	155
Defamation / Privacy Violation	470	103	73	25	0	5
Speculative spirit promotion / Pyramid	400	248	2	1	244	1
Wild rumour	13	7	5	2	0	0
Anti-nation	1	0	0	0	0	0
Fraudulent election	703	0	0	0	0	0
Injustice Advertisement	18	4	1	3	0	0
Obscenity / Violence Text	408	154	75	70	0	9
Obscenity / Violence Sound	0	0	0	0	0	0
Obscenity / Violence material sale	1,961	1,482	5	96	1,347	34
Obscenity / Violence material purchase	240	178	29	149	0	0
Obscenity / Violence material exchanging	371	323	26	143	154	0
Leading unhealthy meeting	583	179	0	22	152	5
Unhealthy chatting	3,004	1,200	4	1,193	3	0
Introducing a place of obscene material	624	249	9	99	131	10
Verbal violence	2,657	1,363	72	1,291	0	0
Prostitution	2	1	0	0	0	1
Obscene still image	2,153	1,743	1,309	364	21	49
Violence still image	78	57	21	30	5	1
Obscene movie	1,328	1,112	487	261	25	339
Violence movie	20	17	6	10	0	1
Obscene game	692	661	592	58	10	1
Violence game	4	0	0	0	0	0
Etc. / Out of classification	1,866	1,537	100	1,430	6	1
Non-deliberation subject	9	0	0	0	0	0
Total	23,477	15,440	2,953	7,517	4,358	612

January 1999—December 1999

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	10,299	7,958	1,178	4,676	2,078	26
Defamation / Privacy Violation	983	110	92	14	4	0
Speculative spirit promotion / Pyramid	513	346	23	175	147	1
Wild rumour	34	11	7	4	0	0
Anti-nation	51	0	0	0	0	0
Fraudulent election	1	0	0	0	0	0
Injustice Advertisement	57	32	20	12	0	0
Obscenity / Violence Text	1,772	572	204	282	79	7
Obscenity / Violence Sound	106	6	0	2	1	3
Obscenity / Violence material sale	3,364	2,923	278	1,255	1,383	7
Obscenity / Violence material purchase	274	194	17	175	2	0
Obscenity / Violence material exchanging	228	192	7	61	124	0
Leading unhealthy meeting	1,859	821	33	375	402	11
Unhealthy chatting	2,079	1,687	35	1,426	225	1
Introducing a place of obscene material	687	325	69	115	140	1
Verbal violence	2,288	1,505	122	1,353	29	1
Prostitution	28	16	0	0	9	7
Obscene still image	2,455	1,328	975	334	19	0
Violence still image	80	51	34	15	2	0
Obscene movie	391	205	152	44	9	0
Violence movie	18	15	10	5	0	0
Obscene game	466	434	239	151	44	0
Violence game	37	3	1	2	0	0
Etc. / Out of classification	1,525	993	69	840	58	26
Non-deliberation subject	12	2	0	0	0	2
Total	29,607	19,729	3,565	11,316	4,755	93

January 1998—December 1998

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	4,012	3,594	1,080	1,522	981	11
Defamation / Privacy Violation	179	97	41	40	15	1
Speculative spirit promotion / Pyramid	927	448	16	300	129	3
Wild rumour	42	18	11	5	1	1
Anti-nation	13	7	2	3	2	0
Fraudulent election	0	0	0	0	0	0
Injustice Advertisement	13	10	8	1	1	0
Obscenity / Violence Text	124	89	37	40	12	0
Obscenity / Violence Sound	346	178	0	0	145	33
Obscenity / Violence material sale	4,043	3,768	1,554	1,558	648	8
Obscenity / Violence material purchase	0	0	0	0	0	0
Obscenity / Violence material exchanging	0	0	0	0	0	0
Leading unhealthy meeting	1,114	635	325	276	30	4
Unhealthy chatting	1,169	990	110	416	451	13
Introducing a place of obscene material	112	76	18	36	22	0
Verbal violence	2,086	1,080	172	759	129	20
Prostitution	0	0	0	0	0	0
Obscene still image	1.266	931	659	232	36	4
Violence still image	3	2	1	1	0	0
Obscene movie	55	38	33	4	1	0
Violence movie	0	0	0	0	0	0
Obscene game	62	61	24	36	1	0
Violence game	1	1	0	1	0	0
Etc. / Out of classification	1,528	652	49	310	287	6
Non-deliberation subject	13	7	0	0	1	6
Total	17,108	12,682	4,140	5,540	2,892	110

January 1997—December 1997

Type of Violation	Number of deliberation	Request of revision				
		Total	Deleting content	Warning	Use suspense	Use cancellation
Copyrights Violation	1,509	1,233	209	807	216	1
Defamation / Privacy Violation	77	48	30	15	3	0
Speculative spirit promotion / Pyramid	0	0	0	0	0	0
Wild rumour	6	6	3	1	2	0
Anti-nation	0	0	0	0	0	0
Fraudulent election	1,826	1	1	0	0	0
Injustice Advertisement	0	0	0	0	0	0
Obscenity / Violence Text	8	8	6	2	0	0
Obscenity / Violence Sound	0	0	0	0	0	0
Obscenity / Violence material sale	1,942	1,738	423	958	343	14
Obscenity / Violence material purchase	0	0	0	0	0	0
Obscenity / Violence material exchanging	0	0	0	0	0	0
Leading unhealthy meeting	0	0	0	0	0	0
Unhealthy chatting	1,112	711	17	422	271	1
Introducing a place of obscene material	0	0	0	0	0	0
Verbal violence	4,470	1,476	69	1,152	255	0
Prostitution	0	0	0	0	0	0
Obscene still image	1,218	768	324	357	85	2
Violence still image	0	0	0	0	0	0
Obscene movie	0	0	0	0	0	0
Violence movie	0	0	0	0	0	0
Obscene game	0	0	0	0	0	0
Violence game	0	0	0	0	0	0
Etc. / Out of classification	1,848	357	20	300	36	1
Non-deliberation subject	0	0	0	0	0	0
Total	14,016	6,346	1,102	4,014	1,211	19

APPENDIX F

Notification of the Commission on Youth Protection (No. 2000-31)

Notification of the Commission on Youth Protection (No. 2000-31)

Under Article 8(1) and 22(2) of *the Juvenile Protection Act*, ICEC classifies a medium material listed below into a harmful-to-youth material and requests CYP to issue a notification of its decision. Hereby, under Article 22(1) of the same Act, CYP issues a notification as follows.

20th September 2000 / Commission on Youth Protection

---

1. The list of the harmful-to-youth medium material: See the table below

2. Obligation

A person who provides the harmful-to-youth medium material listed below is obliged to comply with the harmful-to-youth medium material indication system (Article 14) and should not exhibit or display the medium material for the purpose of selling or renting (Article 17).

3. Penalty

A person who has failed to stick indications on his media materials shall be punished by imprisonment with prison labour for not more than two years or by a fine not exceeding 10 million KRW.

A person who has violated the provisions of Articles 17 (1) shall be punished by imprisonment with prison labour for not more than three years or by a fine not exceeding 20 million KRW.

Table of harmful-to-youth medium (electric communication material)

Serial No.	2000-1736
Title	EXZONE
URL	http://exzone.com
Organisation of Deliberation	ICEC
Deliberation No.	20001725-1
Date of Deliberation	25th August 2000
Reason for Determination	Obscenity

(Resource: CYP. Retrieved August 5, 2002, from http://www.youth.go.kr/environment/default_retrieval.htm)

APPENDIX G

Questionnaire:
The Impacts of the Internet Content Rating System
on the Actual Internet Contents in South Korea

6th January 2003

Dear,

I am writing to you to ask if you would kindly complete the enclosed questionnaire and return it by 10th of February.

This questionnaire aims at surveying the impacts of the Internet content rating system on the actual Internet contents in South Korea. The questionnaire consists of twenty-five questions with four sections which ask about general information, the Internet content rating system, the harmful-to-youth medium material indication system, and rating and labeling respectively.

Your reply will be read only by myself and it will be treated in strict confidence. In any reporting of my work, only aggregate statistics will be presented, so no organisation or individual will be mentioned by name.

I should be most grateful if you would find the time to complete my questionnaire. I am hoping that my work will make a valuable contribution helping to liberalise the South Korean government's policies on the Internet content regulation.

Yours sincerely

Kim, You-seung
yskim@btinternet.com

Ph.D. student
School of Library, Archive and Information Studies
University College London
Gower Street
London
WC1E 6BT

Section I: General Information

Q1. Please state your occupation or job title.

Webmaster	[ ]	Web Programmer	[ ]
Web Contents Developer	[ ]	Web Designer	[ ]

*Other (please state your job title)*_____

Q2. How would you class the Website which you own or work for?

Art	[ ]	Entertainment	[ ]	Organisation	[ ]
Business	[ ]	Health	[ ]	Society/Culture	[ ]
Computing	[ ]	Internet	[ ]	Sport	[ ]
Education	[ ]	News	[ ]	*Other*	[ ]

Q3. What is the age group of your site's target audience? Tick or complete all relevant options.

Children	[ ]	Teenagers	[ ]
Adult	[ ]	The elderly	[ ]

Section II: The Internet Content Rating System

Q4. Have you heard about the Internet content rating system?

Yes [ ] No [ ]

(If YES, please answer to all questions from Q5 to Q10. If NO, please go to Q11)

Q5. If YES, tick or complete all relevant boxes.

ESRB	[ ]	SafeNet system	[ ]
ICRA system	[ ]	SafeSurf	[ ]
Medcertain	[ ]	Safety Online	[ ]
RSACi system	[ ]	None	[ ]

Q6. How confident are you in using the Internet content rating system?

Very confident	[ ]
Fairly confident	[ ]
Not at all confident	[ ]

Q7. The Internet content rating system is an efficient technical solution to protect minors from harmful information on the Internet. Do you agree?

Strongly agree	[ ]	Strongly disagree	[ ]
Agree	[ ]	Unsure / Don't know	[ ]
Disagree	[ ]		

Q8. The Internet content rating system may violate freedom of expression on the Internet. Do you agree?

Strongly agree	[ ]	Strongly disagree	[ ]
Agree	[ ]	Unsure / Don't know	[ ]
Disagree	[ ]		

Q9. Do you agree that a governmental institution should operate the Internet content rating system?

Yes [ ] No [ ] Don't know [ ]

Q10. In your opinion, which of the following organisations do you think ought to operate the Internet content rating system? Tick or complete all relevant options.

Academic Expert Group	[ ]	Internet Industry	[ ]
Government	[ ]	Non-governmental Organisation	[ ]

Section III: The harmful-to-youth medium material indication system

Q11. Have you heard about the harmful-to-youth medium material indication system?

Yes [ ] No [ ]

(If YES, please answer to all questions from Q12 to Q15, If NO, please go to Q16)

Q12. How confident are you in using the harmful-to-youth medium material indication system?

Very confident [ ]
Fairly confident [ ]
Not at all confident [ ]

Q13. Would you classify the harmful-to-youth medium material indication system as an Internet content rating system?

Yes [ ] No [ ] Don't know [ ]

Q14. The harmful-to-youth medium material indication system is an efficient technical solution to protect minors from harmful information on the Internet. Do you agree?

Strongly agree [ ]
Agree [ ]
Disagree [ ]
Strongly disagree [ ]
Unsure / Don't know [ ]

Q15. The harmful-to-youth medium material indication system may violate freedom of expression on the Internet. Do you agree?

Strongly agree [ ]
Agree [ ]
Disagree [ ]
Strongly disagree [ ]
Unsure / Don't know [ ]

Section IV: Labelling and Rating

Q16. At present, do you label your site with any Internet content rating system including the harmful-to-youth medium material indication system? (*If YES, please answer all questions from Q18 to Q25. If NO, please answer to Q17*)

Yes [ ] No [ ]

Q17. If NO, why not?

Unnecessary [ ]
Technical difficulty [ ]
Not informed [ ]

Other (please specify)

_____
_____
_____

Q18. If YES, why do you label your site with the Internet content rating system(s)?

By recommendation(s) [ ]
By my (companie's) own decision [ ]
By legal order(s) [ ]

Other (please specify) _____

Q19. How many Internet content rating systems are you using at present?

1 [ ] 2 [ ] more than 2 [ ]

Please, specify the Internet content rating system(s) which you are using now.

_____

Q20. Did you apply the label to the whole site or to specific pages?

Whole site [ ] Specific pages [ ]

Q21. Have you experienced any technical difficulty concerning rating and labelling on your site?

Yes [ ] No [ ]

Q22. Dose the Internet content rating system provide enough rating categories and descriptors for classifying your site?

Yes [ ] No [ ] Don't know [ ]

Q23. How long in total did it take to label your site?

less than 1 hour	[ ]	4-8 hours	[ ]
1-4 hours	[ ]	more than 8 hours	[ ]

Q24. After labelling your site, has there been any change to your Website's traffic?

None [ ] Increase [ ] Decrease [ ] Don't know [ ]

Q25. Have you ever revised your site's contents in order to get a certain degree of rating?

Yes [ ] No [ ]

Many thanks for answering to the questionnaire.

APPENDIX H

The Questionnaire Sample List

Notes: B = Broken links, **N** = No e-mail address, **UC** = Under construction

Home

Sub-category	No.	Title	URL	E-mail	Etc.
Home	001	e-Buup	http://www.ebuup.co.kr	tkjin@kr.qrio.com	
	002	Sosamo	http://www.sosamo.co.kr	webmaster@sosamo.net	
	003	Consumer Times	http://www.ConsumerTimes.co.kr		B
	004	Web Trust Korea	http://www.WebtrustKorea.org		B
Family	005	Reunion	http://www.reunion.or.kr/	reunion@kwf.or.kr	
	006	Town Space	http://www.townspace.co.kr/	helpdesk@antnet.co.kr	
	007	Good Mom	http://www.goodmom.co.kr/	goodmom@goodmom.co.kr	
	008	SWS	http://www.sws.or.kr/main.asp	bwy1004@sws.or.kr	
Finance	009	Samil Tax	http://www.samiltax.co.kr/		B
Marriage	010	Wedding-i	http://www.weddingi.net/	webmaster@weddingi.net	
	011	TMM	http://www.tmm.co.kr/	master@tmm.co.kr	
	012	Couple Club	http://www.coupleclub.co.kr	webmaster@coupleclub.co.kr	
	013	I Love Wedding	http://www.ilovewedding.com/	wetizen@ilovewedding.com	
Meeting	014	Wowzzim	http://www.wowzzim.com		
	015	ING Love	http://www.inglove.co.kr/	webmaster@inglove.co.kr	
	016	XY in Love	http://www.xyinlove.co.kr	webmaster@mail.xy.co.kr	
	017	Date Net	http://www.datenet.co.kr/	webmaster@datenet.co.kr	
Media	018	Lulu	http://www.lulu.co.kr/		B
Living Information	019	ZON	http://www.zon.co.kr/	master@zon.co.kr	
	020	Korea Interent 114	http://www.hk114.co.kr/	webmaster@hk114.co.kr	
	021	Dizzo Life	http://www.dizzolife.co.kr/		N
	022	Chazri	http://www.chazri.co.kr	webmaster@chazri.net	
Consumer Information	023	Korean Consumer Union	http://www.consumersunion.or.kr/	cukip@chollian.net	
	024	Korea National Council of Consumer Organisations	http://www.consumernet.or.kr	sohyub@consumernet.or.kr	
	025	CACPK	http://www.cacpk.org	cacpk@cacpk.org	
	026	Oh My Oil	http://www.ohmyoil.com		UC
Apartment Living	027	Eunma A.P.T. Community	http://www.eunma.com/	webmaster@eunma.com	
Children	028	Smile of Kids	http://www.kids.co.kr/	shopmaster@kids.co.kr	
	029	Teentoc.com	http://www.teentoc.com	teentoc@teentoc.com	
	030	Totovil	http://www.totovil.co.kr/	webmaster@totovil.co.kr	
	031	Unikids	http://www.unikids.co.kr	unikids1@unitel.co.kr	
Women	032	Women Line	http://www.womenline.com/	womenline@womenline.co.kr	
	033	Patzzi.com	http://www.patzzi.com	webmaster@patzzi.com	
	034	Azoomma.com	http://www.azoomma.com	azoomma@azoomma.com	

	035	Elli Clothes Making	http://happy-elli.com/	elli@happy-elli.com	
Food / Cooking	036	JOY2FOOD	http://www.joy2food.com	webmaster@joy2food.com	
	037	Cook 'n' Joy	http://www.cooknjoy.co.kr	cooknjoy@daesang.co.kr	
	038	Banchan Nara	http://www.banchan.co.kr	banchan@banchan.co.kr	
	039	Hello Cook	http://www.hellocook.com	webmaster@hellocook.com	
Moving	040	The ladder truck society	http://www.sadari114.com	sadari114@sadari114.com	
	041	Z24 Home	http://www.z24.co.kr/move/	webmaster@z24.co.kr	
	042	24Q Moving Service	http://www.24q.co.kr	q24@24q.co.kr	
	043	Good24	http://www.good24.co.kr/	kim@good24.co.kr	
Divorce	044	Divorce.net	http://divorcenet.co.kr/	divorcenet@blue-chip.co.kr	
Parenting	045	MamaPapa	http://www.mamapapa.co.kr	webmaster@mamapapa.co.kr	
	046	Working Mum	http://workingmom.pe.kr		N
	047	Baby Welcom	http://www.babywel.com	help@babywel.com	
	048	0to7	http://www.0to7.com	webmaster@0to7.com	
Rural Living	049	Best Home	http://www.besthome.co.kr/	webmaster@goodsite.net	
	050	Green Home	http://www.greenhome.net/	webmaster@greenhome.net	
Housing	051	How Home	http://www.howhome.co.kr	shopmaster@howhome.co.kr	
	052	Dobae Home	http://www.dobaehome.co.kr	web@dobaehome.co.kr	
	053	Housetopia	http://www.housetopia.co.kr/	hslee@housetopia.co.kr	
	054	Dobae1004	http://www.dobae1004.com	dobae1004@dobae1004.com	
Fashion	055	K-Fashion	http://www.kfashion.co.kr	jenny@kweather.co.kr	
	056	Knit School	http://www.knit-school.co.kr	filpucci@knit-school.co.kr	
	057	My Fashion	http://www.myfashion.co.kr/	info@myfashion.co.kr	
	058	Fashion Plus	http://www.fashionplus.net/	netmaster@fashionplus.co.kr	
Cosmetic	059	Beauty-i	http://www.beautyi.com	webmaster@beautyi.com	
	060	I.B.I	http://www.wakuwaku.co.kr/	webmaster@wakuwaku.co.kr	
	061	Cyber Fashion Academy	http://www.cyfa.co.kr	webmaster@dongahtv.com	
	062	DODO	http://www.dodo.co.kr/	mpark@dodo.co.kr	

Health

Sub-category	No.	Title	URL	E-mail	Etc.
Nursing	063	Chonbuk University, Nurses' school	http://nursing.chonbuk.ac.kr/	nursing@chonbuk.ac.kr	
Organisation	064	National Health Insuramce Corporation	http://www.nhic.or.kr	webmaster@nhic.or.kr	
	065	The Korea Heart Foundation	http://www.heart.or.kr/	heart@heart.or.kr	
	066	Solidarity for People's Health as Right	http://www.konkang.or.kr/	kss0205@kornet.net	

	067	Association of Physicians for Humanism	http://www.humanmed.org	inyeeh@kornet.net	
News & Media	068	MEDIA M	http://www.mediland.co.kr	rep33@mediland.co.kr	
	069	Daily Medi	http://www.dailymedi.com	webmaster@dailymedi.com	
	070	Bokuen News	http://www.bokuen.co.kr/		N
	071	J-Health Care	http://healthcare.joins.com/	joins_healthcare@joins.com	
Diet	072	Health Korea.Net	http://diet.healthkorea.net/	service@mail.healthkorea.net	
	073	Good Diet	http://www.gooddiet.com	gooddiet@gooddiet.com	
	074	Green Diet	http://www.greendiet.co.kr/	greendiet@greendiet.co.kr	
	075	One-shot Diet	http://www.oneshotdiet.co.kr	kmj@oneshotdiet.co.kr	
Alternative	076	Hygiene Korea	http://www.hygiene-korea.com	hey8253@hitel.net	
	077	K.Y 1.2 Eye Centre	http://www.eyehealth.co.kr/	counselor@eyehealth.co.kr	
	078	Alter-medi.com	http://www.altermedi.com	nailkang@altermedi.com	
	079	Food for you	http://www.food4u.co.kr	food4u@food4u.co.kr	
Animal	080	Korean Veterinary Medical Associaton	http://www.kvma.or.kr/	kvma@kvma.or.kr	
	081	Seoul Uni. Veterinary Medical Centre	http://www.vetinfo.org/		B
Beauty	082	Daedong Uni.	http://www.daedong.ac.kr/partho me		B
Hospital	083	Korea Hospital Associtation	http://www.kha.or.kr/	khaweb@kha.or.kr	
	084	Clinic	http://www.clinic.co.kr/	webmaster@clinic.co.kr	
Health	085	Korea Institute for Health & Social Affairs	http://www.kihasa.re.kr/	master@kihasa.re.kr	
	086	Health technology Planning & Evaluation Board	http://www.hpeb.re.kr/		N
	087	OHIS	http://www.ohis.net/		B
	088	Korea Health Industry Development	http://www.khidi.or.kr/	webadmin@khidi.co.kr	
Services	089	Nursing Korea	http://www.nursingkorea.co.kr	parang@interpia.co.kr	
Child	090	Medcity	http://medcity.com/soa.html	webmaster@medcity.com	
Pharmacy	091	Daily Pharm.com	http://www.dreamdrug.com/	kbyoo@dreamdrug.com	
	092	PharmacyOK	http://www.pharmacyok.com/	pharmacyok@pharmacyok.com	
	093	Healthy Neighbour	http://www.drug-info.co.kr/	dasalim@drug-info.co.kr	
	094	Lead Pharm	http://www.leadpharm.com/	webmaster@neovortal.com	
Women	095	OBGYN.net	http://www.obgynkorea.net	webmaster@obgynkorea.net	
	096	CHACARES	http://www.chacares.com	webmaster@chacares.com	
	097	Cyber Breast Cancer Centre	http://www.yubang.com	ohsemin@hotmail.com	
	098	Midwifery Service	http://www.becob.co.kr	agihalme@dreamwiz.com	
Online prescription	099	WOW Doctor	http://www.wowdoctor.co.kr		UC
	100	Care Korea	http://www.carekorea.co.kr	webmaster@carekorea.co.kr	
	101	Medizoa	http://www.medizoa.com		B
	102	Medi101	http://www.medi101.com	neolcg@pop-ms.co.kr	

Web Broadcasting	103	Dr. Crezio	http://www.drcrezio.co.kr/	service@drcrezio.co.kr	
	104	MedTV21	http://www.medtv21.net	webmaster@maxql.com	
Medical Appliances	105	Mediris	http://www.mediris.co.kr/	mediris@mediris.co.kr	
	106	Hi-Doc	http://www.hidoc.co.kr	webmaster@page1.co.kr	
	107	Medisamll.com	http://www.medismall.com		N
	108	Mtongil.com	http://www.Mtongil.com	tongil@tong-il.co.kr	
Medical Doctor	109	Virtual MD	http://www.virtualmd.co.kr	Form Mail	
	110	From Doctor	http://www.fromdoctor.com/	webmaster@fromdoctor.com	
	111	Medi-Gate	http://www.medigate.net/	master@medigate.net	
	112	Be.md	http://www.be.md	webmaster@be.md	
Medical Science	113	The Korean Society of Circulation	http://www.circulation.or.kr/	webmaster@circulation.or.kr	
	114	Mdhouse	http://www.MDhouse.com	webmaster@mdhouse.com	
	115	Medi-Campus	http://www.medicampus.co.kr/	webmaster@medicampus.co.kr	
	116	Dr. MinJu	http://www.drminju.or.kr/	drminju@drminju.or.kr	
Traditional Medical Science	117	Sumac	http://www.sumacpa.co.kr	sumac@sumacpa.co.kr	
	118	Health8	http://www.health8.co.kr/	webmaster@health8.co.kr	
	119	New Medi	http://www.newmedi.com/	newmedi@newmedi.com	
	120	Sasang	http://www.sasang.com/		UC
Mental	121	Counsel24	http://www.counsel24.com/	webmaster@counsel24.com	
	122	Ssijes	http://www.ssijes.com/	webmaster@ssijes.com	
	123	Psycho News	http://www.psychonews.co.kr/	master1@psychonews.co.kr	
	124	Internet Choimyun	http://www.choimyun.co.kr/	webmaster@choimyun.co.kr	
Diseases	125	Regrow.co.kr	http://nobald.co.kr/	regrow@hanmail.net	
	126	Influenza	http://www.dokgam.com	webmaster@medtv21.net	
	127	Goodbye Nemo	http://www.goodbyenemo.co.kr	nemo@goodbyenemo.co.kr	
	128	Oh My Tuck	http://www.ohmytuck.com	zusanli@hanmail.net	
Fitness	129	O2run	http://www.o2run.com	webmaster@o2run.com	
Company	130	Health Info	http://www.healthinfo.co.kr/		N
	131	Medidas	http://www.medidas.co.kr	admin@ubcare.co.kr	

Game

Sub-category	No.	Title	URL	E-mail	Etc.
Developer	132	Jamie	http://www.jamie.co.kr	Webmaster@jamie.co.kr	
Gambling	133	Internet Lotto	http://www.lotto.co.kr	info@lotto.co.kr	
	134	Tigerpools Sports TOTO	http://www.tigerpools.co.kr/	Form Mail	
	135	Miss TOTO	http://www.misstoto.co.kr/	info@misstoto.co.kr	

	136	Sport Betting	http://www.sporbet.com/		B
Gamer	137	Korea Pro Gamer League	http://www.kpgl.net/	kpgl@kpgl.net	
News & Media	138	Game Sarang	http://game.sarang.net/		B
	139	PCGAME	http://www.pcgame.co.kr/		N
Badok	140	Neostone	http://www.neostone.co.kr	neostone2002@vanhouse.co.kr	
Video Game	141	Game Spot Korea	http://gamespot.zdnet.co.kr/	games@korea.cnet.com	
	142	Game Shot	http://www.gameshot.net/	webmaster@gameshot.net	
	143	Demo Land	http://www.demoland.co.kr	webmaster@demoland.co.kr	
	144	Game News	http://www.game-news.co.kr		N
Internet	145	Game Dory	http://www.gamedory.com/	webmaster@gnation.co.kr	
	146	Net Marble	http://www.netmarble.net/	help@netmarble.co.kr	
	147	Free Golf	http://www.freegolf.co.kr/	game@freenix.co.kr	
	148	Crazy Arcade	http://www.crazyarcade.com/	nexoncontact@nexon.co.kr	
Card Game	149	Seven Card	http://www.7card.net		N
Casino	150	Joy4you	http://www.joy4you.com	webmaster@joy4you.com	
	151	Casino City	http://www.acecasinocity.com	help_korean@casinoquery.com	
	152	Casino Korea	http://www.casinodynastykorea.com/	info@casinodynastykorea.com	
	153	Flash Casino Game	http://www.Luck4u.co.kr	hws@korea.com	
Puzzle	154	Battle Puzzle	http://www.puzpuz.com/	webmaster@puzpuz.com	

Science

Sub-category	No.	Title	URL	E-mail	Etc.
Engineering	155	KT Link	http://www.ktlink.com	webmaster@ktlink.com	
	156	Gongdori - Special Site for Engineers	http://www.gongdori.com	gongdori@hye.co.kr	
	157	WELDNET	http://www.weldnet.co.kr	weldnet@weldnet.co.kr	
	158	Cons-Info	http://www.cons-info.com/main.htm	kmsohn@cons-info.com	
Instruments and Supplies	159	Science119.com	http://www.science119.com	sales@science119.com	
	160	Lab Nutz	http://www.labnutz.com		B
Educational Resources	161	NDSL	http://ndsl.or.kr/		B
Organisation	162	Korea Database Promotion Centre	http://www.dpc.or.kr/	heung200@dpc.or.kr	
	163	Korea National Science Museum	http://www.nsm.go.kr/	webadmin@nsm.go.kr	
	164	International Robot Olympiad	http://www.iroc.org	seoul@iroc.org	
	165	Korea Science Foundation	http://www.ksf.or.kr/	webmaster@ksf.or.kr	
Agriculture	166	NIAST	http://www.niast.go.kr/	kmkim@rda.go.kr	
	167	Korea Agriculture Science Digital Library	http://lib.rda.go.kr	kslee@lib.rda.go.kr	

	168	National Agricultural Mechanizaiton Research Institute	http://www.namri.go.kr/	haki@rda.go.kr	
	169	Korea Rural Economic Institute	http://www.krei.re.kr/	webadm@krei.re.kr	
Physics	170	Korean Physical Society	http://www.kps.or.kr	webmaster@mulli.kps.or.kr	
	171	Information Center for Physics Research	http://icpr.snu.ac.kr/	icmail@icpr.snu.ac.kr	
	172	Heureka Science Class	http://user.chollian.net/~msjys	msjys@chollian.net	
Social Sciences	173	Society @nd Culture	http://www.sociology.pe.kr/	sociology@yu.ac.kr	
	174	Dept. of Cultural Anthropology, Hanyang Univ.	http://www.anthronet.org/		N
	175	Korean Ancient Historical Society	http://sanggo.mokpo.ac.kr/	webmaster@mnum.mokpo.ac.kr	
	176	BOKJI.net	http://www.bokji.net/	bokjinet@bokji.net	
Biology	177	KRIBB	http://www.kribb.re.kr	admin@kribb.re.kr	
	178	Bioinformatics Information	http://www.bioinformatics.pe.kr/course/	sywon@bioinformatics.pe.kr	
	179	The Zoological Society of Korea	http://www.zsk.or.kr	bjku@zsk.or.kr	
	180	Biochemical Society	http://www.biochem.or.kr/	bsrk@gly.biochem.or.kr	B
Meth	181	MathNet	http://www.mathnet.or.kr	nsadmin@mathnet.or.kr	
	182	Korea Mathematical Society	http://www.kms.or.kr/	kms@www.kms.or.kr	
	183	StatEdu	http://www.statedu.com/	stat@statedu.com	
Earth	184	Korea Meteorological Administration	http://www.kma.go.kr/index.html	webmaster@kma.go.kr	
	185	Global Generation 21	http://www.gg21.co.kr		N
Astronomy	186	Astro Korea	http://www.astrokorea.com	kwon572@astrokorea.com	
	187	Sky Watcher	http://www.sky39.com/thesky/skywatcher/main.htm	sky@sky39.com	
	188	The Korean Space Science Society	http://ksss.or.kr/	ksss@ksss.or.kr	
	189	Astro Note	http://astronote.org	webmaster@astronote.org	
Chemistry	190	Chemical Engineering Reserch Information Centre	http://infosys.korea.ac.kr/	w3master@cheric.org	
	191	Info Chems.com	http://www.infochems.co.kr	Form Mail	
Environment	192	Enviornemt and Pollution Research Group	http://www.ecoi.or.kr/	enthink@chollian.net	
	193	KONETIC	http://www.konetic.or.kr/	onlyone@emc.or.kr	
	194	Webzine Megalam	http://megalam.chollian.net		B

Education and Reference

Sub-category	No.	Title	URL	E-mail	Etc.
Education	195	EDU	http://www.edu.co.kr/	webmaster@edu.co.kr	
	196	Njoy School	http://www.njoyschool.net		N
	197	eTest	http://www.etest.co.kr	help@etest.co.kr	
	198	Go Campus	http://www.gocampus.co.kr/		

Traffic Inforamtion	199	Free Way	http://www.freeway.co.kr/	sysop@freeway.co.kr	
	200	KATIS	http://www.katis.co.kr/	emmaus@katis.co.kr	
Library	201	Korean Assembly Library	http://www.nanet.go.kr/	w3@nanet.go.kr	
	202	Puchon Braille Library	http://www.pcl.or.kr/	webmaster@pcl.or.kr	
	203	Korea Braille Library	http://kbll.or.kr/	kbl@kbll.or.kr	
	204	419Revolution Digital Library	http://library.419revolution.org	webmaster@mail.419revolution.org	
Museum	205	Samsung Kids Museum	http://www.samsungkids.org	khyuna@samsung.co.kr	
	206	Museum Tour	http://www.museumtour.co.kr	jujin@noricom.co.kr	
	207	Jung-Juyoung Cyber Museum	http://www.asanmuseum.com	jychung@hyundai.com	
	208	Post Museum	http://www.postmuseum.go.kr	webmaster@postmuseum.go.kr	
Encyclopedia	209	Dusan EnCyber	http://www.encyber.com/	ad@encyber.com	
Dictionaries	210	Trems.co.kr	http://www.terms.co.kr/	admin@terms.co.kr	
People	211	People 21	http://www.people21.co.kr/	master@people21.co.kr	
Experts	212	e-KnowHow	http://e-knowhowbank.co.kr/	knowhow@eknowhowbank.com	
Information	213	Alchane	http://www.alchane.com/	alchane@alchane.com	
Map	214	Free Map	http://www.freemap.net/	freemap@ktit.com	
	215	CyberMap	http://www.cybermap.co.kr	imap@cybermap.co.kr	
	216	Map114	http://www.map114.com	map114@map114.com	
	217	onM@P	http://www.onmap.co.kr/main.asp	terage@dohwa.co.kr	

News and Media

Sub-category	No.	Title	URL	E-mail	Etc.
Organisation	218	Korea Press Foundation	http://www.kpf.or.kr	media@kpf.or.kr	
	219	Kwanhun Club	http://www.kwanhun.com/	kwanhun@kwanhun.com	
	220	LG Press Net	http://www.lgpress.org	mijune@office.lg.co.kr	
News	221	Kyosu.net	http://www.profs.co.kr	webmaster@kyosu.net	
	222	iNews24	http://www.inews24.com	webmaster@inews24.com	
	223	Campus weekly of Yonsei Uni.	http://chunchu.yonsei.ac.kr/	webmaster@chunchu.yonsei.ac.kr	
	224	CNU Today	http://www.chonnam.ac.kr/~cnutoday/		B
Online	225	Say World	http://www.sayworld.net/	webmaster@sayworld.co.kr	
	226	Pressian	http://www.pressian.com	webmaster@pressian.com	
	227	News Boy	http://www.newsboy.co.kr	webmaster@newsboy.co.kr	
	228	Buregi Report	http://breport.com.ne.kr	supilzip@hotmail.com	
Internet Broadcasting	229	Crezio	http://www.crezio.com/	webmaster@crezio.com	
	230	Imcine	http://www.imcine.com	ahadvro@hanmail.net	

	231	CHATV	http://www.chatv.co.kr/	info@chatv.co.kr	
	232	Wildnet	http://www.wildnet.co.kr	eco21@wildnet.co.kr	
Megazine	233	KMPA	http://www.kmpa.co.kr/		B
	234	Magazine World	http://www.magazineworld.co.kr/	magazine@magazineworld.co.kr	
	235	Moda News	http://www.modanews.com	Modanews@modanews.com	
	236	PC Line	http://www.pcline.co.kr/	webmaster@pcline.co.kr	

Business

Sub-category	No.	Title	URL	E-mail	Etc.
Management	237	BizLine	http://www.bizline.co.kr	webmaster@bizline.co.kr	
	238	Wise Info	http://www.wisedb.co.kr/	wiseinfonet@wiseinfonet.com	
	239	Top Zone	http://www.topzon.co.kr/		B
	240	jYOU-net	http://www.jyou.co.kr		B
Education and Training	241	Biz Academy	http://www.biz-academy.co.kr	21educon@korea.com	
	242	Global Knowledge	http://www.globalknowledge.co.kr/	jahaekoo@globalknowledge.co.kr	
	243	OPE	http://www.ope.co.kr	ope@ope.co.kr	
	244	Need Feel	http://www.needfeel.com/	webmaster@richschool.co.kr	
International Business and Trade	245	Korea Trade News	http://www.tradenews.net/	webmaster@tradenews.net	
	246	Trade Campus	http://www.tradecampus.com	dblee@kotis.net	
	247	Korea Trade Commission	http://www.ktc.go.kr/	anobb@mocie.go.kr	
Financial Service	248	Money Today	http://www.moneytoday.co.kr	webmaster@moneytoday.co.kr	
	249	Money Plus	http://www.moneyplus.co.kr/		N
	250	Millionaire Club	http://www.starhana.com	unseg@hanmail.net	
Organisation	251	Korea Women Entrepreneurs Associtaion	http://www.womanbiz.or.kr		N
	252	KIWA	http://www.ikiwa.or.kr	kiwa2001@kornet.net	
Labour	253	Nozo.net	http://www.nozo.net		
	254	Nodong OK	http://www.nodong.or.kr	master@nodong.or.kr	
	255	Good Morning	http://www.goodnosa.com	kns1974@goodnosa.com	
Marketing	256	MA Com	http://www.macoms.com		N
	257	BoBu Net	http://www.bobunet.com/	webmaster@bobunet.com	
	258	Cyber Marketing School	http://www.marketingschool.com	webmaster@marketingschool.com	
	259	DailyComms	http://www.dailycomms.com	newsmaster@dailycomms.com	
Venture	260	SKY Venture	http://www.skyventure.co.kr	webmaster@skyventure.co.kr	
	261	University Venture Forum	http://www.uventure.org	webmaster@khan.co.kr	

	262	Venture Net	http://venture.smba.go.kr		N
	263	Idea Plaza	http://www.ideaplaza.co.kr/	ideainfo@ideaplaza.co.kr	
Real Estate	264	Ten Community	http://www.ten.co.kr/	webmaster@ten.co.kr	
	265	Real Estate Today	http://www.Rtoday.com	webmaster@rtoday.com	
	266	Budongsan.com	http://www.Budongsan.com	Budongsan@budongsan.com	
	267	Best House 114	http://www.besthouse114.com	master@besthouse114.com	
Business	268	EB News	http://www.ebn.co.kr	webmaster@ebn.co.kr	
	269	Cyber Publishing	http://www.publishing21.com	Webmaster@publishing21.com	
	270	Now Press.com	http://www.nowpress.com		B
Services	271	Text Writing	http://www.textwriting.com	webmaster@textkorea.com	
	272	Writers	http://www.writers.co.kr	writers@writers.co.kr	
	273	007visa.com	http://www.007visa.com	webmaster@iminlawfirm.com	
E-commerce	274	e-Corporation.co.kr	http://www.e-corporation.co.kr/	webmaster@e-corporation.co.kr	
	275	KorChamBiz	http://www.korchambiz.net		N
	276	Siri	http://www.siri.co.kr	Form Mail	
	277	BBX	http://www.bbx.co.kr	bbx@bbx.co.kr	
Small Business	278	Tokebi	http://www.tokebi.co.kr	tokebi@chollian.net	
	279	Bizini.com	http://www.bizini.com	webmaster@bizini.com	
	280	Bonabank	http://www.bonabank.com	bona@bonabank.com	
Knowledge and Information	281	Koreaform	http://www.koreaform.co.kr/	webmaster@koreaform.co.kr	
	282	Bizform	http://www.bizforms.co.kr	sun@bizforms.co.kr	
	283	eBizup	http://www.ebizup.com		N
	284	Briefing	http://www.briefing.co.kr	webmaster@infocast.co.kr	
Establishment	285	PC	http://www.smmechatronics.com		N
	286	OK-Sneakers	http://www.ok-sneakers.co.kr	ok-sneakers@hanmail.net	
	287	Oh My Biz	http://www.ohmybiz.co.kr	ohmybiz@ohmybiz.co.kr	
	288	Woyaco	http://woyaco.com	woyaco@woyaco.com	
Employment	289	Job Korea	http://www.jobkorea.co.kr/	helpdesk@jobkorea.co.kr	
	290	Incruit	http://www.incruit.com	incruit@incruit.com	
	291	Recruit	http://www.recruit.co.kr	webmaster@recruit.co.kr	
	292	Adecco Korea	http://www.adecco.co.kr	webmaster@adecco.co.kr	
Consulting	293	IBS Consulting Group	http://www.ibs.co.kr/	webmaster@ibs.co.kr	
	294	e-MIT Korea	http://mitc.co.kr/	pkr@e-mit.co.kr	
	295	Image Making	http://www.imagesense.co.kr	iml@imagesense.co.kr	
	296	MB Zone	http://www.mbzon.com	webmaster@mbzon.com	
Investing	297	Neovision Community	http://www.neovision.co.kr/	hana@neovision.co.kr	

	298	CybersDaq	http://www.cybersdaq.com/		B
Companies	299	NICE	http://www.nice.co.kr	webmaster@nice.co.kr	
	300	Jinyoung Sweet Persimmon.	http://www.jinyoung.co.kr	webmaster@jinyoung.co.kr	
	301	Happy Name	http://www.happyname.co.kr	happyname@happyname.co.kr	

Society

Sub-category	No.	Title	URL	E-mail	Etc.
Military	302	Mizzle	http://www.mizzle.com/	webmaster@mizzle.com	
	303	McnLove	http://www.mcnlove.net	love@rokmcn.net	
	304	Military Review	http://www.militaryreview.com	webmaster@militaryreview.com	
Organisation	305	Free Get	http://www.ksrd.or.kr	Form Mail	
	306	21NGO	http://www.21ngo.or.kr	21ngo@21ngo.or.kr	
	307	World Vision	http://www.worldvision.or.kr	wv@worldvision.or.kr	
Labour	308	Info-Sanjae	http://www.info-sanjae.co.kr	webmaster@info-sanjae.co.kr	
Culture	309	Webzine Zunk	http://www.zunk.com/		B
	310	Think-Culture	http://www.think-culture.com		B
	311	Ing Love	http://www.inglove.co.kr	webmaster@inglove.co.kr	
	312	Jammy	http://www.jammy.net		B
Crime	313	Korean Institute of Criminology	http://www.kic.re.kr/	webmaster@mail.kic.re.kr	
Law	314	Legal Information SOL	http://www.sol-law.net	hwl@lawyers.co.kr	
	315	Bubdori	http://www.bubdori.co.kr/		N
	316	Zone4u	http://www.thezone4u.net	webmaster@thezone4u.net	
	317	Law Korea	http://www.lawkorea.com/	Webmaster@voin.com	
Welfare	318	Santa Nara	http://www.santanara.net	santa@santanara.net	
	319	Dana-Nuri.com	http://www.dananuri.com		N
	320	Social Worker Net	http://socialworker.co.kr/	worker@socialworker.co.kr	
People	321	Honey Hoeny	http://honeyhoney.new21.net		B
	322	NCT Club	http://nctclub.com	webmaster@nctclub.com	
	323	YORI	http://www.yori.co.kr	webmaster@yori.co.kr	
	324	Chun-Hyang	http://www.chunhyang.or.kr	webmaster@chunhyang.or.kr	
Social Security	325	HIRA	http://www.hira.or.kr/	hira@hira.or.kr	
Social Movement	326	CCEJ	http://www.ccej.or.kr	mannam7@ccej.or.kr	
	327	Citizens' Action Network	http://www.ww.or.kr	member@mail.ww.or.kr	
	328	Dae-an TV	http://www.daean.org/		B
	329	Webzine With	http://www.mywith.net/	pyo@mywith.net	
History	330	Korea Photo	http://www.koreanphoto.co.kr	webmaster@koreanphoto.co.kr	

	331	Anti Japan	http://members.tripod.lycos.co.kr/antyjapan	parkjoohyun@korea.com	
Issue	332	Issue Today	http://www.issuetoday.com	webmaster@issuetoday.com	
	333	Cyber Tok-do	http://www.tokdo.tv/	cyber@tokdo.com	
	334	Union Community	http://www.unionzone.com		N
	335	Panmunjom	http://panmunjom.co.kr	webmaster@panmunjom.co.kr	
Disable	336	KEPAD	http://www.kepad.or.kr	Webmaster@kepad.or.kr	
	337	Hanbeot	http://www.hanbeot.or.kr/	move@hanbeot.or.kr	
Politics	338	PiBKorea	http://www.pibkorea.co.kr	info@pibkorea.co.kr	
	339	Polcom.co.kr	http://www.polcom.co.kr	polcom@polcom.co.kr	
	340	N-politics	http://www.npolitics.co.kr		N
	341	Internet Politics	http://www.internetpolitics.co.kr	shim4822@unitel.co.kr	
Religion	342	World Religion	http://www.religion.co.kr/		B
	343	HD Jongkyo	http://www.hdjongkyo.co.kr/	tongsim@hdjongkyo.co.kr	
	344	Nanum Community	http://www.nanumcafe.net	webmaster@fgtv.com	
	345	Chun-bul-dong	http://www.buddhasite.net	sysop@buddhasite.net	
Death	346	Funeral21	http://www.funeral21.co.kr/	funeral21@funeral21.co.kr	
	347	Cyber Tomb	http://www.cybertomb.co.kr		B
Philosophy	348	Sophie	http://www.sophie.co.kr/	hyeonamsa@sophie.co.kr	
Surreal	349	Minaisa Club	http://www.herenow.co.kr/	herenow@korea.com	
Environment	350	Webzine Chenvi	http://www.chenvi.com		B
	351	Korean Federation Environment Movement	http://www.kfem.or.kr	web@kfem.or.kr	
	352	Fulssi	http://www.fulssi.or.kr/	fulssi@fulssi.or.kr	
	353	Enviropia	http://www.enviropia.co.kr/	webmaster@enviropia.co.kr	

Shopping

Sub-category	No.	Title	URL	E-mail	Etc.
Electronics	354	My Digital	http://www.mydigital.co.kr/	kbh@mydigital.co.kr	
	355	Internet T-Zone	http://www.tzone.co.kr		UC
	356	TM21	http://www.tm21.com	webmaster@tm21.com	
	357	49Shopping	http://49shopping.co.kr/	webmaster@49shopping.co.kr	
Home	358	Deconara	http://www.deconara.com	himsh@deconara.com	
	359	How Home	http://www.howhome.co.kr	shopmaster@howhome.co.kr	
	360	Aura83	http://www.aura83.com/main.html	quilt@aura83.com	
	361	Sujee1004	http://www.sujee1004.com/	webmaster@sujee1004.com	
Health	362	Care Mall	http://www.caremall.co.kr	webmaster@caremall.co.kr	
	363	Health Mall	http://www.kunkangmall.co.kr/	webmaster@kunkangmall.co.kr	

	364	Aroma 'n' Life	http://www.aromanlife.com/	aroma@aromanlife.com	
	365	Smile Foot	http://www.smilefoot.com	smilefoot@smilefoot.com	
Purchase	366	09Zone	http://www.09zone.com/	help@09zone.com	
	367	MY09.COM	http://www.my09.com/	mallmaster@my09.com	
	368	Cap Ssada	http://www.capssada.com	webmaster@capssada.com	
	369	09Gate	http://www.09gate.com	webmaster@09gate.com	
Flowers	370	Postlab	http://www.postlab.co.kr		B
	371	Art Box	http://www.nartbox.com		N
	372	Hello! Santa	http://www.hellosanta.co.kr/	hslee@hellosanta.co.kr	
	373	iWOW	http://iwow.co.kr	iwow@iwow.co.kr	
Rental	374	Rental Enjoy	http://www.rentalenjoy.com		B
	375	E-rent	http://www.erent.co.kr/	smile@erent.co.kr	
	376	Rental Plaza	http://www.rental-plaza.com		UC
	377	Hi-tech Rental	http://www.rentop.co.kr	rentop@rentop.com	
Book	378	Fox Book	http://www.foxbook.com/		B
	379	School Book	http://www.schoolbook.co.k		B
	380	WJ Book Club	http://www.wjbookclub.com	mallmaster@woongjin.com	
	381	Libro	http://www.libro.co.kr/	webmaster@libro.co.kr	
Stationery	382	K School	http://www.kschool.co.k		B
	383	New Office	http://www.new-office.co.kr	newoffice@new-office.co.kr	
	384	Office Man	http://www.officeman.co.kr/	officeman@officeman.com	
	385	Office Plus	http://www.officeplus.co.kr	yes@officeplus.co.kr	
Cultural Item	386	Picture Plus	http://www.pictureplus.co.kr/		UC
	387	All CD	http://www.allcd.co.kr		B
	388	Gana Art Shop	http://www.artshop.co.kr	webmaster@ganaart.com	
	389	Neo-art Mall	http://www.neoartmall.com	sayall@neoartmall.com	
Search	390	Find All	http://www.findall.co.kr	webmaster@findall.co.kr	
	391	My Margin	http://www.mymargin.com/		N
	392	Hal-pan.com	http://halpan.com	halpan@halpan.com	
	393	Best Buyer	http://www.bestbuyer.co.kr	webmaster@bbr.co.kr	
Video, Film	394	Movie Empire	http://www.movieempire.co.kr	webmaster@movieempire.co.kr	
	395	DVD Nara	http://www.dvdnara.net	webmaster@dvdnara.net	
	396	FineAV.com	http://www.fineav.com	webmaster@fineAV.com	
	397	Video Unlimited	http://www.viu.pe.kr/		B
Daily Necessities	398	In hand	http://inhand.co.kr	inhand@inhand.co.kr	
	399	Masulgage	http://masulgage.com/	Form Mail	
	400	Kidsmoon	http://kidsmoon.com	Form Mail	
	401	Puppy & Marie	http://mariedog.co.kr	mariepuppy@empal.com	

Adult	402	Korea Sex Toy	http://www.koreasextoy.com	help@koreasextoy.com	
	403	Love Haja	http://www.lovehaja.co.kr	lovehaja@lovehaja.co.kr	
	404	Sex in Door	http://www.sexindoor.com	master@sexindoor.com	
	405	Nude119	http://www.nude119.co.kr	moonkr@nude119.co.kr	
Sport	406	Daegun Sport	http://www.dickey.co.kr/	Form Mail	
	407	Asiana Sport	http://www.anasports.co.kr	Form Mail	
	408	Dream Sport	http://www.dreamspoz.com	angel@dreamspoz.com	
	409	Espoz	http://espoz.com		B
Food	410	HRS Shopping Mall	http://www.hrs.co.kr	webmaster@hrs.co.kr	
	411	Tea	http://www.ebuytea.com		B
	412	Uja Love	http://myhome.naver.com/ujalove/	ujasarang@hanmail.net	
	413	e-Gohyang	http://www.e-gohyang.com	webmaster@egohyang.com	
Child	414	eDolls	http://www.edolls.co.kr	edolls@edolls.co.kr	
	415	Kids Box	http://www.kidsbox.co.kr	webmaster@kidsbank.co.kr	
	416	FYKO Shopping Mall	http://www.fyko.co.kr/	webmaster@fyko.co.kr	
	417	Koma Nara	http://www.komanara.com	webmaster@komanara.com	
Women	418	Soho Dance	http://www.sohodance.com	help@sohodance.com	
	419	See & Choice	http://www.see-choice.co.kr	webmaster@jungbo114.com	
Music	420	Changgo	http://www.changgo.com/	support@changgo.com	
	421	Phonograph	http://www.phono.co.kr/	webmaster@phono.co.kr	
	422	Music Medicine	http://www.music2life.com/	center@music2life.com	
	423	My Music	http://www.mymusic.co.kr	privacy@mymusic.co.kr	
Car	424	Carway	http://www.carway.co.kr/	carway@carway.co.kr	
	425	iComes,com	http://www.iComes.com	webmaster@icomes.com	
	426	Libero	http://www.libero.co.kr	webmaster@neoplan.co.kr	
	427	eLuxury Car	http://www.eluxurycar.co.kr	info@eLuxurycar.co.kr	
Toy, Game	428	Toy DC	http://www.toydc.com	toydc@toydc.com	
	429	Gana Toy	http://www.ganatoy.com	shenker@netsgo.com	
Shopping Mall	430	Woori Home Shopping	http://www.woori.com	master@woori.com	
	431	Inter-park	http://www.interpark.com	cpo@interpark.com	
	432	Easy Club	http://www.easyclub.co.kr/	webmaster@easyclub.co.kr	
	433	nFree Zone	http://www.nfreezone.com		B
Used Item	434	Gabas	http://www.gabas.co.kr	gabas@gabas.co.kr	
Computer	435	iLogix	http://www.ilogix.co.kr	webmaster@ilogix.co.kr	
	436	PC Out	http://www.pcout.com/		B
	437	Compuzone	http://www.compuzone.co.kr	compuzone@compuzone.co.kr	
	438	Click OK	http://www.clickok.co.kr	doumi@skdtod.com	
Special Product	439	WEBBEN	http://korea.webben.co.kr	shopmaster@webben.co.kr	

	440	OK DZ	http://OKDZ.com		N
	441	Jeju Shopping	http://www.jejushopping.co.kr/	webmaster@jazzercise.co.kr	
	442	Onggi-Hanmadang	http://www.onggimadang.co.kr	webmaster@ onggimadang.co.kr	
Ticket	443	Ticket Link	http://www.ticketlink.co.kr	webmaster@ticketlink.co.kr	
	444	Happy Money	http://www.happymoney.co.kr	happy@happymoney.co.kr	
	445	iTicket	http://www.iticket.co.kr	webmaster@iticket.co.kr	
	446	Ticket4848	http://www.ticket4488.co.kr	ticket4488@ticket4488.co.kr	
Fashion	447	Cyshion	http://www.cyshion.com		B
	448	Fashion Plus	http://www.fashionplus.co.kr/	customer@fashionplus.co.kr	
	449	Y Shirts Net	http://www.yshirts.net	webmaster@yshirts.net	
	450	Fashion21c	http://www.fashion21c.com	webmaster@fashion21c.com	
Cosmetic	451	i-CoCo	http://www.i-coco.co.kr	help@i-coco.co.kr	
	452	Beauty Eve	http://www.beautyeve.net/	webmaster@beautyeve.net	
	453	Gagaelle	http://www.gagaelle.com	gagaelle@gagaelle.com	
	454	Makeup Mall	http://www.makeupmall.co.kr/	info@makeupmall.com	

Sport

Sub-category	No.	Title	URL	E-mail	Etc.
Golf	455	Golf291	http://www.golf291.co.kr/	golf@golf291.co.kr	
	456	Golf1	http://www.golf1.co.kr	golf1@golf1.co.kr	
	457	The Golf	http://www.thegolf.co.kr/	thegolf@thegolf.co.kr	
	458	iwatchgolf	http://www.iwatchgolf.com	webmaster@digitalview.co.kr	
Organisation	459	KAPA	http://www.apa.or.kr/	webmaster@walking.or.kr	
	460	National Council of Sport for All	http://www.sports-net.or.kr/	nacosa@sportal.or.kr	
Basketball	461	Street Basketball	http://www.streetbasketball.com/		B
	462	ILoveBasketball	http://www.ilovebasketball.net/	webmaster@ilovebasketball.net	
	463	Basketball2i	http://www.basketball2i.com/	bk2i@sports2i.com	
	464	Korean Basketball League	http://www.kbl.or.kr/	webmaster@kbl.or.kr	
News / Media	465	Wow Sport	http://www.wowsports.co.kr	spo@spo.co.kr	
Lacrosse	466	Korean Lacrosse Association	http://www.lacrosse.or.kr	mjkim405@hotmail.com	
Rugby	467	Korea Rugby Union	http://rugby.sports.or.kr/	rugby@sports.or.kr	
Motor Sport	468	F1 Race	http://www.f1race.com		B
	469	F1 All	http://www.f1all.net	Form Mail	
	470	Paddock Club	http://www.paddockclub.co.kr/	racing@paddockclub.co.kr	
Martial Art	471	Muye Love	http://www.muyelove.com		UC
	472	Fighter	http://www.fighter.co.kr/	fighter@catm.co.kr	

	473	Kyong-Dang	http://flowolf.hihome.com		N
	474	Mooyerang	http://mooyerang.co.kr/	Webmaster@mooyerang.co.kr	
American Football	475	KAFA	http://www.kafa.org/	kafa@kafa.org	
Volleyball	476	Korea Volleyball Association	http://www.kva.or.kr/	kva@kva.or.kr	
Bowling	477	Bowling Korea	http://www.bowling.co.kr/	webmaster@bowling.co.kr	
	478	Bowling Camp	http://www.bowlingcamp.com/	bowling2@bowlingcamp.com	
	479	Webzine Bowl Park	http://www.bowlpark.com		B
	480	Bowling Maul	http://www.bowlingmaul.co.kr/	uingan@yahoo.co.kr	
Water Sport	481	Water Ski	http://www.waterski.co.kr/	webmaster@waterski.co.kr	
Swimming	482	Water Safety Zone	http://myhome.dreamx.net/arota/	watesafe@yahoo.co.kr	
	483	Unifin	http://www.unifin.oo.co.kr/	s1swim@unitel.co.kr	
	484	Swim Doctor	http://www.swimdoctor.co.kr/	swimdoctor@swimdoctor.co.kr	
	485	Finflier	http://www.finflier.com/	flier@finflier.com	
Snowboard	486	Riderz	http://www.RiderzShop.com	riderz@riderzshop.com	
	487	Boarders Zone	http://www.boarderszone.com	kimjunbeom@boarderszone.com	
	488	Chicken Salsd	http://www.chickensalad.co.kr	webmaster@chickensalad.co.kr	
Skateboard	489	Eszone	http://www.eszone.com/	jbogo@dreamwiz.com	
	490	Flateen Skateboarding	http://www.flateen.com	master@flateen.com	
Skating	491	Road Riders	http://www.roadriders.co.kr		B
Squash	492	Squash.co.kr	http://www.squash.co.kr/		B
Skiing	493	Ski World	http://www.skiworld.co.kr/	webmaster@skiworld.co.kr	
	494	Ski 114	http://www.ski114.com/		
	495	Internet Ski Magazine	http://www.skimagazine.co.kr/	webmaster@skimagazine.co.kr	
	496	Ski Page	http://www.skipage.co.kr/	skipage@hanmail.net	
Sport Medical Science	497	Sport & Health	http://www.sportskorea.net/health		
Riding	498	Kwangju Equestrian Club	http://www.horsy.co.kr/	kseungma@horsy.co.kr	
	499	Equestrian	http://sportsmuseum.co.kr/term/equestrian.htm	webmaster@sportsmuseum.co.kr	
	500	C & C	http://www.horsenet.co.kr	horsenet@webtown.org	
Cycle	501	Bike Love	http://www.bike.or.kr/	webmaster@bike.or.kr	
	502	Bike Nara	http://www.ectop.co.kr/	ectop@ectop.co.kr	
	503	Webzine Mountain Bike	http://www.mountainbike.co.kr		N
Baseball	504	Baseball2i	http://www.baseball2i.com	bb2i@sports2i.com	
	505	Yagoo Korea	http://www.yagoo.co.kr/	yagoo@yagoo.co.kr	
	506	My MLB	http://www.mymlb.co.kr/		B
	507	Yagoo114	http://www.yagoo114.com/	khpark@joypia.com	
Olympics	508	Gangwon2010	http://www.gangwon2010.org	webmaster@mail.pyeongchang2010.com	

	509	Olympic Info	http://juneun.hihome.com/		N
Athletic sport	510	Korea Modern Pentathlon Federation	http://www.pentathlon.or.kr/	1993kang@daum.net	
Extreme Sport	511	Xmania	http://www.xmania.tv	skpark@bnl.co.kr	
	512	Xvil	http://www.xvil.tv	xvil@xvil.co.kr	
Triathlon	513	Pusan Triathlon Club	http://www.pusan3club.com/	kudoree@hanmail.net	
Gymnastics	514	World Dance Sport Academy	http://www.krdance.com/	admin@krdance.com	
	515	Kangwon GYM	http://gym-kw.or.kr/		B
Football	516	Soccer4u	http://www.soccer4u.co.kr	w3master@soccer4u.co.kr	
	517	Soccer Bank	http://www.soccerbank.co.kr/	webmaster@mail.soccerbank.co.kr	
	518	Soccero	http://www.soccero.com		N
	519	Soccer Mania	http://soccermania.co.kr		N
Table tennis	520	Champion	http://www.champion.co.kr/	Form Mail	
Taekwondo	521	MOOTO	http://www.taekwon.net/	webmaster@mooto.com	
	522	Taekwon Line	http://www.taekwonline.com		N
	523	Taekwonvil	http://www.taekwonvil.com	webmaster@eculture.co.kr	
	524	Taekwon World	http://winwinsports.co.kr	ilsun@winwinsports.co.kr	
Tennis	525	Tennis Korea	http://www.tennis.co.kr	tennis@tennis.co.kr	
	526	Hingis	http://hingis81.naweb.cc/	webmaster@hingis.pe.kr	
	527	Tennis Plaza	http://www.tennisplaza.co.kr	tennis@tennisplaza.co.kr	
	528	Pusan Open	http://www.pusanopen.org/	k5778@chollian.net	
Fantasy	529	Sposdaq	http://www.sposdaq.co.kr	webmaster@sports.co.kr	
	530	VS Sport Betting	http://www.vs.co.kr/		B
Hockey	531	Jim Peak	http://www.jimpaek.com/	customers@jimpaek.com	

Kids and Teens

Sub-category	No.	Title	URL	E-mail	Etc.
News, Media	532	KYBC	http://www.kybc.org	webmaster@kybc.org	
	533	CINDY the Perky	http://www.cindy.co.kr/	Form Mail	
People	534	KYCI	http://www.kyci.or.kr	webmaster@kyci.or.kr	
Health	535	NoSmoke.or.kr	http://www.nosmoke.or.kr	uhlee@kah.or.kr	
	536	Child and Adolescent Psychiatric Clinic	http://childpsy.webpd.co.kr	childpsy@drchoi.pe.kr	
Entertainment	537	Wa Joa	http://www.wajoa.co.kr/	webmaster@wajoa.com	
Art	538	Donghwa Nara	http://www.donghwanara.com/	webmaster@playe.co.kr	

Entertainment

Sub-category	No.	Title	URL	E-mail	Etc.
TV	539	TVnTV	http://www.tvntv.com		UC
Advertisement	540	WOW CF	http://www.wowcf.net/		B
Catoon	541	Postnut	http://www.postnut.com	info@postnut.com	
	542	EComiX	http://www.ecomix.co.kr	admin@ecomix.co.kr	
	543	Korea Pen Cartoon	http://www.koreapen.com	koreapen@koreapen.com	
Video	544	CineLine	http://www.cineline.co.kr	cineline@cineline.co.kr	
	545	Video Wave	http://www.vwave.co.kr/	vwave@vwave.co.kr	
	546	Video Korea	http://www.videokorea.com	videop@kornet.net	
	547	WAVi	http://www.wavi.co.kr/	webmaster@bestgold.co.kr	
Animation	548	Best Anime	http://www.bestanime.co.kr/	bestanime@bestanime.com	
	549	Club WOW	http://www.clubwow.com/	webmaster@clubwow.com	
	550	Ghost Net	http://ghostnet.co.kr		N
	551	Anipy	http://www.Anipy.com	exit99@hompy.com	
Online Card	552	Dear You	http://www.dearyou.com	Form Mail	
	553	Magic EZ	http://www.magicez.com	webmaster@magicez.com	
	554	Boombo.com	http://www.boombo.com	webmaster@minesoft.co.kr	
	555	Cizmail	http://www.ciz.co.kr	help@cizmedia.com	
Entertainer	556	Star Korea	http://www.starkorea.co.kr	master@starkorea.co.kr	
	557	SOLIGOL	http://www.sorigol.co.kr	webmaster@sorigol.co.kr	
	558	Knson-city	http://www.knsoncity.com	webmaster@knson.co.kr	
Movie	559	Joy Cine	http://www.joycine.com	webmaster@joycine.com	
	560	Cine Seoul	http://www.cineseoul.com	webadmin@cineseoul.com	
	561	No Cut	http://www.nocut.co.kr	nocut@nocut.co.kr	
	562	Movist	http://www.movist.co.kr	master@movist.co.kr	
Web Broadcast	563	eStars	http://www.estars.co.kr	webmaster@estars.co.kr	
	564	Sorea	http://www.sorea.co.kr	webmaster@sorea.com	
	565	OKCAST	http://www.okcast.com/		B
	566	VAVATV	http://www.vavatv.com		B
Webzine	567	Cultizen	http://www.cultizen.co.kr	cultizen@cultizen.co.kr	
	568	Hamsung21	http://my.dreamwiz.com/hamsung21/	hamsung21@hanmail.net	
	569	Hikin	http://www.hikin.com	hikin@hikin.com	
Humour	570	Ggame	http://www.ggame.net	home114@kebi.com	
	571	Miso-mail	http://www.misomail.co.kr	MisoMail@Misomail.co.kr	
	572	Puha	http://www.puha.co.kr	puha1@puha.co.kr	
	573	Yupgy.com	http://www.yupgy.com/	yupgy@orgio.net	

Events	574	Wooa	http://www.wooa.net	webmaster@wooa.net	
	575	Joy Link	http://www.joylink.co.kr		N
	576	Eye Gift	http://www.eyegift.co.kr/		B
	577	Helloluck.com	http://www.helloluck.com	helper@helloluck.com	
Company	578	Amuse Korea	http://www.amusekorea.co.kr/	webmaster@amusekorea.co.kr	
	579	TP Entertainment	http://www.thinkpeople.net		N
	580	CJ Entertainment	http://www.cjent.co.kr	cjemaster@cj.net	
	581	Shin-Sung	http://www.totalstage.net	SHIN0714@hitel.net	

Leisure and Hobby

Sub-category	No.	Title	URL	E-mail	Etc.
Horse Racing	582	Korea Race	http://www.korearace.com	koshin@gamsoft.co.kr	
	583	Gumvit	http://www.gumvit.com/	gumvit@gumvit.com	
	584	Horse Nara	http://www.horsenara.com	webmaster@emutant.co.kr	
Theme Park	585	Korean Folk Village	http://www.koreanfolk.co.kr/	master@kreanfolk.co.kr	
	586	Lotte World	http://www.lotteworld.com	lotty@lotteworld.com	
	587	Bugok Hawaii	http://www.bugokhawaii.co.kr/	webmaster@bugokhawaii.co.kr	
	588	Dream Land	http://www.dreamland.co.kr/	dreaml0@dreamland.co.kr	
Reading	589	ILKSAE	http://www.ilksae.co.kr	ilksae@yahoo.co.kr	
	590	Book Cosmos	http://www.bookcosmos.com	webmaster@bookcosmos.com	
	591	Libzone.com	http://www.libzone.co.kr/	cho519@libzone.com	
	592	New Book	http://www.newbook.co.kr	webmaster@worldpia.co.kr	
Climbing	593	OK Mountain	http://www.okmountain.com/	okoutdoor@okoutdoor.com	
	594	iALP	http://www.ialp.co.kr/		B
Recreation	595	IDance	http://www.idance.co.kr	idance@spaceillusion.com	
	596	Dance114	http://www.dance114.com	master@dance114.com	
	597	YJT Dance Sport School	http://yjtdance.co.kr		B
Motor Cycle	598	SLGI	http://www.slgi.co.kr	leems@alphamotors.co.kr	
	599	8mmnet.com	http://www.8mmnet.com		B
	600	Motor Fashion	http://www.motorfashion.net/	motorfashion@hotmail.com	
Model	601	Hobby Tek	http://www.hobbytek.co.kr	hobbytek@hobbytek.co.kr	
	602	Joy Hobby	http://www.joyhobby.co.kr	joyhobby@joyhobby.net	
	603	Hobby Times	http://www.hobbytimes.co.kr/		B
Baduk	604	Badook TV	http://www.onbadook.com/	webmaster@onbadook.com	
	605	Badook World	http://www.badukworld.co.kr/	www@badukworld.net	

	606	WeGoBaduk	http://www.wegobaduk.com/	biz@wegobaduk.com	
	607	Baduk.to	http://www.baduk.to/		B
Boating	608	Koryoin	http://www.koryoin.co.kr	webmaster@koryoin.co.kr	
Photo	609	iMedia	http://www.iMedia.co.kr	help@imedia.co.kr	
	610	Korea Album	http://www.korea-album.co.kr	kgac@korea-album.co.kr	
	611	Colala	http://www.colala.co.kr	colala@colala.co.kr	
	612	Zoomin	http://www.zoomin.co.kr/	webmaster@zoomin.co.kr	
Stone	613	Suseok World	http://www.suseokworld.co.kr	artpro@artpro.co.kr	
	614	Korean Orchid	http://www.seoulorchid.co.kr		B
Collection	615	Tube Ticket Collection	http://cj56.hihome.com/		N
	616	Fly Land	http://www.flyland.co.kr		UC
	617	Hwa-dong	http://www.hwadong.com/	master@hwadong.com	
	618	Barbie	http://barbie86.hihome.com/	barbie86@bcline.com	
Planting	619	Beautiful Garden	http://www.greenbiz.co.kr	baraz@netian.com	
	620	Nan Love	http://www.nan.co.kr	nan@nan.co.kr	
	621	Green Flora	http://www.greenflora.com		N
	622	Won Nan	http://www.nanyasijang.com/		UC
Pet	623	WithPet.com	http://www.withpet.com/	Form Mail	
	624	Nature21.com	http://www.nature21.com	webmaster@nature21.com	
	625	PETV	http://www.petv.co.kr/	webmaster@petv.co.kr	
	626	Pet City	http://www.petcity.co.kr	petcity@petcity.co.kr	
Leisure	627	Run Diary	http://www.rundiary.co.kr		N
	628	Nexfree	http://www.nexfree.com	webmaster@nexfree.com	
	629	Joy View	http://www.joyview.com	joyview@joyview.com	
	630	Match	http://www.match.co.kr/	Form Mail	
Travel	631	Vision Tour	http://www.visiontour.com/	webmaster@visiontour.com	
	632	Travel21	http://www.travel21.co.kr/	cheju21@hananet.net	
	633	Essen Tour	http://www.essentour.co.kr	Form Mail	
	634	Travel cafe	http://www.travelcafe.co.kr/	honey-tour@hanmail.net	
Fortunetelling	635	Saju Campus	http://sajucampus.com	webmaster@sajucampus.com	
	636	Yuksul.com	http://www.yuksul.com/	webmaster@yuksul.com	
	637	Fortune 8282	http://www.fortune8282.com	operator@fortune8282.co.kr	
	638	Gung-Hap	http://www.gunghap.com	gunghap@kebi.com	
Audio	639	Audio Journal	http://www.audiojournal.co.kr	audiojournal@yahoo.com	
	640	Hi-Fi Net	http://hifinet.co.kr/	webmaster@hifinet.co.kr	
	641	Audio Camp.net	http://www.audiocamp.net	webmaster@audiocamp.net	

Car	642	iComes	http://www.iComes.com	webmaster@icomes.com	
	643	Good Car	http://www.gogoodcar.com	rf130@netian.com	
	644	Web4Car	http://www.web4car.co.kr/	webmaster@web4car.co.kr	
	645	Carmily	http://www.carmily.org	carmily@samsungfire.com	
Toy	646	Kitty Maina	http://myhome.hananet.net/~nalrari		B
Aviation	647	X Camp	http://www.xcamp.co.kr	xcampcontact@nexon.co.kr	
	648	Iisan Hobby	http://www.ilsanhobby.com/	ilsanhobby@yahoo.co.kr	

Art

Sub-category	No.	Title	URL	E-mail	Etc.
Architectur	649	Korean Institute of Architects	http://www.arick.or.kr/	webmaster@arick.or.kr	
	650	Archforum	http://www.archforum.com/	webmaster@archforum.com	
	651	Archplaza	http://www.a21.co.kr	witharch@a21.co.kr	
	652	Wood Pioneer Society	http://www.wpskorea.org/	woodlee9@snu.ac.kr	
Performing Art	653	GALCHAE	http://www.kin.co.kr/	galchae@galchae.co.kr	
	654	Yettz.com	http://www.yettz.com/	march@yettz.com	
	655	Comedy TV	http://www.comedycenter.co.kr		N
	656	Musical	http://www.musical.co.kr	webmaster@ssace.com	
Craft	657	Art Flower	http://www.artflower.pe.kr/	mania@artflower.pe.kr	
	658	Orange Ballon	http://user.chollian.net/~ldco/	ldco@chollian.net	
	659	Komgi	http://www.komgi.co.kr	webmaster@komgi.co.kr	
	660	Craft Korea	http://www.craftkorea.org	craft@craftkorea.org	
Design	661	Magazine Design House	http://www.design.co.kr		N
	662	Ggumi.com	http://www.ggumi.com	webmaster@ggumi.com	
	663	Design DB.com	http://www.designdb.com	kidp@kidp.or.kr	
	664	Colour World	http://www.colorworld.pe.kr	sekchounji@hanmail.net	
Literature	665	Critics 21	http://www.critics21.com		B
	666	Munhak Review	http://munhak.review.co.kr/	webmaster@review.co.kr	
	667	Julie Luv	http://www.julieluv.com/	jluv@julieluv.com	
	668	Webzine NOVEL	http://www.novel.co.kr/	webnovel@novel.co.kr	
Photo	669	Digieye	http://www.digieye.co.kr	webmaster@digieye.co.kr	
	670	Photo-i.net	http://www.photoi.net	webmaster@photoi.net	
	671	Photo Man	http://www.photoman.co.kr/	photo@photoman.co.kr	
	672	Photocom Korea	http://www.photocom.co.kr/	reoman@reocamera.co.kr	

Visual Art	673	Artin	http://www.artin.com/	Form Mail	
	674	Gana Art	http://www.ganaart.com	webmaster@ganaart.com	
	675	e-Gallery	http://www.egallery.co.kr	admin@egallery.co.kr	
	676	Farrang.com	http://www.farrang.com	farrang@farrang.com	
Music	677	Lets Music	http://www.letsmusic.com/	lets@letsmusic.com	
	678	Musicpia	http://www.musipia.com/		N
	679	M-Shock.com	http://www.m-shock.com	webmaster@m-shock.com	
	680	Oimusic	http://www.oi.co.kr/	privacymaster@oi.co.kr	
Humanities	681	SAYAGA	http://www.sayaga.net/	samil1@samilpatent.co.kr	
Illustration	682	Shin's Human Illustration	http://shisweb.mr4u.com	shisweb@hanmail.net	
	683	Computer Illustration	http://kr.geocities.com/animation kr		B
Magazine, Webzine	684	MILLE21	http://www.mille21.com		N
	685	Ifdream	http://www.ifdream.net	ifdream@ifdream.net	
Traditional Art	686	Chon Hyanh	http://chonhyang.com		N
	687	Chonbuk	http://culture.chonbuk.kr/		B
	688	Hahoe Mask Museum	http://www.tal.or.kr	tal@tal.or.kr	
	689	Korean Garden	http://www.jongwon-koreangarden.com		

The Internet

Sub-category	No.	Title	URL	E-mail	Etc.
WWW	690	Multiro	http://www.multiro.co.kr	info@link.co.kr	
	691	Web Track	http://www.webtrack.co.kr	track4u@webtrack.co.kr	
	692	Go! Webmaster	http://www.runwebmaster.com	kcas@kcas.co.kr	
	693	Websdaq	http://www.websdaq.com		B
Organisation	694	KIBA	http://www.kiba.or.kr	kiba@kiba.or.kr	
	695	WPC	http://www.weblicense.or.kr	w3master@erionet.com	
News, Media	696	eChannel	http://www.ech.co.kr	webmaster@digilife.tv	
	697	Channel-IT	http://www.channelit.co.kr	webmaster@ssexy.net	
	698	Webmania	http://www.webmania.co.kr/	webmaster@webmania.co.kr	
	699	Korea Internet	http://korea.internet.com/	partner@korea.internet.com	
Domain	700	Domains.co.kr	http://www.domains.co.kr/	domain@asadal.com	
	701	Domain Mega-Bank	http://www.DomainMegabank.com	W3master@Domainmegabank.com	
	702	Dodong	http://www.dodong.com	baby@dreamwiz.com	
	703	TO DOT TV	http://www.dottvpeople.tv	tvwebmaster@dottvpeople.tv	

Messenger	704	Digito	http://www.digito.com	some@digito.com	
	705	See Friend	http://www.seefriend.com		B
	706	Digiworks	http://www.fnpoint.com	onesound@korea.com	
Wireless Internet	707	EasyM.com	http://www.easyM.com	korea@easym.com	
	708	Wireless Community	http://www.wirelesscommunity.org		N
	709	Korean Multinet	http://www.koreamultinet.com	webmaster@koreamultinet.com	
	710	Mint	http://www.mymint.net		B
Cyber Culture	711	LAS21	http://www.las21.com	consulting@las21.com	
Web Service	712	OPus	http://www.opus.co.kr/	webmaster@opus.co.kr	
	713	PinkWeb	http://www.pinkweb.co.kr	goodgames@goodgames.co.kr	
	714	Web Sell	http://websell.co.kr/		N
	715	Site Market	http://www.sitemarket.co.kr	info@softvalley.co.kr	
Software	716	Zzagn Bomulsum	http://joywooga.id.ro	webmaster@zzagnbomulsum.com	
	717	Magic Gate GruGru	http://www.guruguru.co.kr	guruguru@gretech.com	
	718	Oh My Soft	http://www.omysoft.com	webmaster@omysoft.com	
	719	Start Korea	http://startkorea.com	webmaster@startkorea.com	
Web TV	720	Internet TV	http://www.intvnet.com	info@intvnet.com	
	721	TCOM.net	http://www.tcomnet.co.kr	webmaster@tcomnet.co.kr	
	722	Korea Web TV	http://www.kebtv.com	webmaster@kebtv.com	
	723	Will Search	http://www.willsearch.co.kr		N
Web Hosting	724	Web Hard	http://www.webhard.co.kr	http://www.webhard.co.kr	
	725	Zoi.net	http://www.zoi.net	zoinet@zoi.net	
	726	Disk Tower	http://www.disktower.com	info@cubesys.co.kr	
Internet Business	727	Mail Bank	http://www.mailbanking.co.kr	help@mailcaster.co.kr	
	728	Sabiz	http://sabiz.co.kr	sabiz@sabiz.co.kr	
	729	O2Some	http://www.o2some.net	o2somecom@o2some.net	
Internet Fax	730	Faxizen	http://www.faxizen.com	kyk518@tronwell.net	
Internet Telephone	731	WOW Call	http://www.wowcall.com	helpdesk@wowcall.com	
	732	Telefree	http://www.telefree.co.kr	leety@telefree.co.kr	
	733	iNew Phone	http://www.inewphone.co.kr	entel@030317.com	
	734	Easy Bell	http://www.easybell.com	wmaster@easybell.com	
E-Mail	735	YUPOST.COM	http://www.yupost.com	webmaster@yupost.com	
	736	Mailjoa	http://www.mailjoa.co.kr		B
	737	Same ID	http://www.sameid.com/		B
Searching	738	Nagaja	http://nagaja.co.kr	webmaster@nagaja.co.kr	
	739	Fivecats.com	http://www.5cats.com		B
Programming	740	iRound	http://www.iround.co.kr	info@biz-valley.com	

	741	ProcessQ	http://www.processq.org	webmaster@processq.org	
	742	JSP School	http://www.jspschool.com/	vans@shinbiro.com	
	743	JSP Master	http://www.jspmaster.com/	totwi@msn.com	

Computer

Sub-D	No.	Title	Web address	E-mail	etc.
CAD	744	Autodesk	http://www.autodesk.co.kr	jaehyang.lim@peopleware.co.kr	
	745	BuzzsawKorea.com	http://www.buzzsawkorea.com		B
	746	CADCom Korea	http://www.cadcamkorea.com	cadcam@cadcamkorea.com	
Virtual Reality	747	Neo-idea	http://www.neoidea.com	master@neoidea.com	
	748	VR360	http://www.VR360.co.kr		B
	749	GameBee	http://www.gamebee.co.kr		N
	750	Battle Top	http://www.battletop.com		B
	751	MGame	http://www.mgame.com	service@wizgate.com	
Education	752	CSERIC	http://cseric.cau.ac.kr	webmaster@cseric.or.kr	
Graphic	753	School eWeb	http://www.schooleweb.com		N
	754	Perfect C.G Link	http://cglink.co.kr/	info@cglink.co.kr	
	755	2D Tools	http://www.2dtools.com		
	756	CG Land	http://www.cgland.com	member@cgland.com	
News, Media	757	eTech Korea	http://www.etechkorea.info/	etechkorea@etechkorea.info	
	758	Bit Daily.Com	http://www.bitdaily.com	webmaster@itchosun.com	
	759	DataNet	http://www.datanet.co.kr	Form Mail	
	760	SV News	http://www.svnews.com/		B
Data Communication	761	KoreaNetworkers	http://www.koreanetworkers.com	kn_agency@koreanetworkers.com	
Data Format	762	Trio	http://trio.co.kr/	trio@trio.co.kr	
	763	XML Lab	http://www.xmlab.com	sysop@ipentec.co.kr	
	764	One Step XML	http://xml.css.co.kr/	webmaster@css.co.kr	
Robotics	765	Robot Soccer	http://www.robot-soccer.co.kr/	webmaster@posco.co.kr	
Mutimedia	766	Neo Paradigm	http://www.neoparadigm.com		B
	767	Better Face	http://www.betterface.co.kr		B
	768	The Happy	http://www.thehappy.pe.kr	jeongsu@hanmail.net	
	769	Consulting Group T.A.G.	http://www.tag.co.kr	tag@tag.co.kr	
Group	770	MDSC	http://myhome.shinbiro.com/~mdsc		B
Security	771	Hacker's Lab	http://www.hackerslab.com	webmaster@hackerslab.com	
	772	Linux Security	http://www.linuxsecurity.co.kr	webmaster@linuxsecurity.co.kr	

	773	Security Zone	http://zone.securewiz.net		N
	774	SecureKR	http://www.securekr.com/		B
Software	775	Web Team	http://www.webteam.co.kr	lonelyhero@wisefn.com	
	776	Software Club	http://www.swclub.net	hsjo@isd.co.kr	
	777	Cool PT	http://www.coolpt.com	Form Mail	
	778	WOW Free	http://www.wowfree.net/	webmaster@wowfree.net	
System	779	Kiss Mac	http://www.kissmac.com	webmaster@kissmac.com	
	780	Hotline Factory	http://www.hotlinefactory.com		B
	781	HanMac Software	http://www.hanmac.com	webmaster@hanmac.com	
Phonetics	782	ACT Valley	http://www.actvalley.com	solution@actvalley.com	
Job	783	MCSE Korea	http://www.mcse.co.kr/	admin@mcse.co.kr	
	784	Green Computer Art School	http://www.00zz.com		B
Inforamtion and Document	785	Power Manual	http://manual.sio.net/		UC
	786	Korea Bench	http://www.kbench.co.kr/	webmaster@kbench.com	
	787	PC Line	http://www.pcline.co.kr/	webmaster@pcLine.co.kr	
	788	How PC	http://www.howpc.com/	jksun@howow.com	
Publishing	789	Younjin.com	http://www.youngjin.com	dannyhong@youngjin.com	
	790	Infopub	http://www.infopub.co.kr	webmaster@infopub.co.kr	
	791	Hanbit	http://www.hanbitbook.co.kr	webmaster@hanbitbook.co.kr	
Consulting	792	Good Hyun	http://goodhyun.com	Form Mail	
	793	Entrue Consulting	http://www.entrue.com	Form Mail	
Computer Science	794	School of Computer Science, Chunbuk Uni.	http://cs.chonnam.ac.kr/		N
	795	KAST	http://www.freechal.com/ksatcom		B
Network	796	Korea Networkers	http://www.koreanetworkers.com	kn_agency@koreanetworkers.com	
	797	Network Camp	http://www.networkcamp.co.kr	webmaster@networkcamp.co.kr	
	798	Fore Net	http://www.forenet.co.kr	admin@forenet.co.kr	
	799	KCWAY	http://www.kcway.co.kr		B